DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN LA EMPRESA T&S. COMP. TECNOLOGÍA Y SERVICIOS S.A.S., EN LOS PROCESOS DE APOYO, MISIONALES Y ESTRATÉGICOS, BASADO EN LA NORMA ICONTEC ISO 27001:2013

MAYRA ALEJANDRA VARGAS GARCÍA
ANDRÉS FELIPE ZUBIETA DAZA

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2017

DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN LA EMPRESA T&S. COMP. TECNOLOGÍA Y SERVICIOS S.A.S., EN LOS PROCESOS DE APOYO, MISIONALES Y ESTRATÉGICOS, BASADO EN LA NORMA ICONTEC ISO 27001:2013

MAYRA ALEJANDRA VARGAS GARCÍA
ANDRÉS FELIPE ZUBIETA DAZA

Proyecto de Grado para optar por el título de Especialista en Seguridad Informática

Asesora
Lorena Ocampo Correa
Ingeniera de Sistemas

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2017

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá, 3 de marzo 2017

CONTENIDO

LISTA DE FIGURAS

pág.

LISTA DE CUADROS

pág.

LISTA DE TABLAS

pág.

LISTA ANEXOS

pág.

GLOSARIO

ACTIVO: recursos, elementos e información que tienen valor y son vitales para el correcto desarrollo de las actividades de la organización.[1]

AMENAZA: circunstancia de un incidente no deseado, que puede atentar o provocar impactos adversos y capaz de aprovechar fallas de los sistemas de la organización.[2]

ANÁLISIS DE RIESGOS: proceso de identificación, valoración y tratamiento de los riesgos, determinando el origen del riesgo y su nivel, para generar salvaguardas que los mitiguen.[3]

BACKORDER: personas encargadas de la demanda del cliente cuando un producto o servicio es superior a la capacidad de la empresa para suministrarlo.

CONTRAMEDIDA: prácticas establecidas por la organización para mitigar los riesgos que puedan afectar los activos de información.[4]

CONTROL: mecanismos como políticas, procedimientos y prácticas adoptados por las organizaciones para mantener los riesgos identificados por debajo del nivel del riesgo asumido.[5]

DESASTRE: evento natural o provocado que produce afectación en las operaciones o servicios de la organización de manera significativa.[6]

IMPACTO: magnitud de pérdidas ocasionadas por amenazas que puede generar un alto costo para las organizaciones como modificación, divulgación, destrucción no autorizada de información.[7]

---

[1] EL PORTAL DE ISO 27001 EN ESPAÑOL, ISO 27000. [Online]. [Consultado 25 de febrero de 2017]. Disponible en: http://www.iso27000.es/glosario.html
[2] Ibíd.,
[3] Ibíd.,
[4] Ibíd.,
[5] Ibíd.,
[6] Ibíd.,
[7] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Glossary of Key Information Security Terms. NISTIR 7298. Impact. pág. 90. Traducido por los autores.

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: serie de eventos no deseados que generan una violación o amenaza inminente a la seguridad de la información y tienen una probabilidad significativa de comprometer las actividades del negocio.[8]

INVENTARIO DE ACTIVOS: lista de activos de la organización que hacen parte del Sistema de Gestión de la Información y que necesitan ser protegidos de potenciales riesgos.[9]

PARTES INTERESADAS: personas involucradas que tienen interés en las decisiones y actividades de la organización.[10]

PROBABILIDAD: oportunidad de ocurrencia de un evento de seguridad de la información.[11]

RIESGO: posibilidad de que las amenazas exploten vulnerabilidades producidas en las operaciones de la organización causando pérdidas o daños a los activos de información.[12]

VULNERABILIDAD: debilidad o susceptibilidad de un activo de información a ser explotado o atacado por una o más fuentes de amenaza.[13]

[8] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, ISO/IEC 27000. Términos y definiciones. pág. 5.
[9] EL PORTAL DE ISO 27001 EN ESPAÑOL, ISO 27000. [Online]. [Consultado 25 de febrero de 2017]. Disponible en: http://www.iso27000.es/glosario.html
[10] Ibíd.,
[11] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Glossary of Key Information Security Terms. NISTIR 7298. Probability. pág. 147. Traducido por los autores.
[12] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Glossary of Key Information Security Terms. NISTIR 7298. Risk. pág. 161. Traducido por los autores.
[13] EL PORTAL DE ISO 27001 EN ESPAÑOL, ISO 27000. [Online]. [Consultado 25 de febrero de 2017]. Disponible en: http://www.iso27000.es/glosario.html

INTRODUCCIÓN

La revolución tecnológica que se ha presenciado en el mundo desde el comienzo de la historia de las comunicaciones, ha impresionado de una forma exorbitante a la sociedad. A causa de esto, se ha hecho necesaria la búsqueda de nuevas tecnologías para el avance y progreso de las empresas para generar crecimiento y desarrollo en el país.

Las empresas en la actualidad, se han visto enfrentadas a mantenerse en las tendencias tecnológicas del mercado para obtener beneficios y lograr el aumento de su productividad. Por esta razón, ante la gran cantidad de información que emplean y la gran facilidad para almacenarla, la información se ha convertido en una de las herramientas más esenciales dentro de las empresas y la buena administración de ésta depende del éxito en las actividades y proyectos que se promuevan en la organización.

Un tema de gran importancia en una organización es la seguridad informática, ésta debe ir alineada con los avances tecnológicos debido al crecimiento de los delitos informáticos que se van presentando a medida del tiempo, y el cual ha provocado daños irreparables y ha generado grandes pérdidas para las empresas víctimas de ataques cibernéticos. Como consecuencia de esto, se ha hecho necesario salvaguardar y proteger la información de la apropiación ilegal de personas que pretenden sacar provecho de vulnerabilidades del gran sistema de información que manejan.

Por tal motivo, se desarrollará este proyecto en la empresa T&S COMP. Tecnología y Servicios S.A.S, en la cual se pretende realizar un diseño del Sistema de Gestión de Seguridad de la Información (SGSI), basado en la norma ISO 27001:2013, en los Procesos de Apoyo, los cuales están compuestos por: Compras y Almacén, Facturación y Recaudo, Gestión Humana y Sistemas, los procesos Misionales compuestos por: Comercial y Servicios; y los procesos Estratégicos compuestos por Gestión Gerencial y Gestión de Calidad.

T&S COMP. Tecnología y Servicios S.A.S. es una empresa colombiana prestadora de servicios de tecnología con más de 10 años de experiencia en reparación, mantenimiento preventivo y correctivo, y soporte de equipos EPSON en empresas del Estado. Debido a los grandes clientes que la empresa les brinda servicios, se hace necesario implementar un SGSI para la protección de los datos el cual se tiene como reto incrementar la capacidad para descubrir y mitigar amenazas, recuperarse de ataques y actualizar su infraestructura obsoleta que pone en riesgo la información.

1. FORMULACIÓN DEL PROBLEMA

Hoy en día, las pequeñas empresas generan grandes cantidades de información, que es almacenada en diferentes medios como: correos electrónicos, archivos físicos, discos ópticos, memorias USB, entre otros; y debe suministrarse a personal de la empresa para diferentes labores. Por esta razón, en las PYME no se tienen buenas prácticas de Seguridad de la Información y existe la probabilidad que se produzcan incidentes que generen pérdida de información sensible, afectando la imagen de la empresa y la continuidad del negocio.

La empresa T&S COMP. Tecnología y Servicios S.A.S ha ido creciendo en el sector de los servicios tecnológicos y ha obtenido gran prestigio por parte de sus clientes, en especial de las empresas del estado que son su mayor target de negocio. Actualmente, la entidad no maneja un programa referente a la seguridad informática, se ha querido diseñar, pero por temas de tiempo y disponibilidad de los ingenieros no ha sido posible el desarrollo del Sistema de Gestión de la Seguridad de la Información. Debido a esto, se ha ido postergando cada vez más su diseño y futura implementación, causando que la empresa este expuesta amenazas y riesgos, generando costos en caso de que se presente algún incidente de seguridad que la empresa no tiene contemplado.

Por lo tanto, un diseño de un programa de Gestión de la Seguridad de la Información permite identificar que fallas presenta la empresa actualmente a nivel de seguridad informática para poder mejorar cada uno de los procesos y evitar futuros ataques.

¿Cómo se puede establecer la integridad, disponibilidad y confidencialidad de la información en un modelo de negocio orientado a la prestación de servicios tecnológicos?

2. JUSTIFICACIÓN

Con el uso de las computadoras y por la gran cantidad de información que las empresas manejaban en el pasado, la gestión de los documentos se automatizó, y la forma de almacenarla pasó de estar en un soporte físico a ser digitalizado. Esta invención facilitó que miles de empresas en el mundo, realizaran la administración de sus registros de manera dinámica y sencilla.

Gracias a las grandes transformaciones y ventajas que la tecnología ofrece, también trae consigo cambios que afectan los sistemas de información como los ataques informáticos. Este es un tema que para muchas empresas son irrelevantes y no han comprendido lo valiosa que es su información. Uno de los errores más notables que en las empresas se cometen, es pensar que su información no es de interés de nadie y, por lo tanto, no fortalecen sus sistemas de seguridad para salvaguardar la información; lo cual da como resultado una infraestructura tecnológica vulnerada y puede ser el blanco de muchos ciberdelincuentes para obtener información sensible.

Según Jon Parkes, Vicepresidente mundial de Preventa de Intel Security, "En el 2020 habrá en el mundo entre 15 y 16 billones de dispositivos y tienen que comunicarse. Nuestro negocio es ver cómo esto se hace de una manera segura"[14]. Si bien es cierto, el gran progreso que en un futuro presentarán las Tecnologías de la Información y las Comunicaciones, requiere de un gran esfuerzo por concientizar a las PYME de la importancia y los desafíos que se enfrentan en temas de seguridad por las nuevas tecnologías y las nuevas vulnerabilidades de las que son el principal blanco de los atacantes cibernéticos. Por tal motivo, es sumamente importante generar un acercamiento con las empresas para concientizarlas del valor de resguardar la información sensible que se encuentra almacenada y, que en efecto, es transmitida por elementos y sistemas de información que día a día están expuestos a vulnerabilidades que se presentan con nuevos ataques informáticos.

Como consecuencia de esto, el propósito del proyecto es realizar una concientización, diseño y posterior implementación de un Sistema de Gestión de Seguridad Informática en la empresa T&S COMP. Tecnología y Servicios S.A.S. "T&S es una empresa integradora de servicios y tecnología con más de 10 años de experiencia en el mercado colombiano"[15], a pesar que maneja servicios de tecnología no tiene diseñado un SGSI.

[14] PORTAFOLIO, 'La seguridad informática se contrajo 15 % en ventas'. [Online] [Consultado el 25 de abril de 2016]. http://www.portafolio.co/negocios/la-seguridad-informatica-se-contrajo-15-ventas

[15] T&S COMP. TECNOLOGÍA Y SERVICIOS S.A.S. Generalidades de la empresa. [Online] [Consultado el 25 de abril de 2016]. http://tyscomp.com/nosotros/

Por temas de tiempo, la empresa se enfoca en su entorno de negocio, dejando a un lado el tema de la seguridad de la información. Por esta razón, es importante primero diseñar el Sistema de Gestión de Seguridad de la Información teniendo en cuenta que la empresa maneja contratos de servicio con entidades estatales que brindan información confidencial para uso exclusivo de la empresa y, en cualquier momento, pueden tener algún incidente de seguridad que comprometa tanto la información confidencial de sus clientes como la de la empresa.

En vista que ningún sistema es seguro, este proyecto permitirá a la empresa promover un ambiente de ciberseguridad con mejores prácticas, orientándola a acciones que permitan la integridad, confidencialidad y disponibilidad de su información, con el objetivo que se logre brindar mayor confianza a sus clientes al momento de desarrollar sus actividades.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un Sistema de Gestión de Seguridad de la Información en la empresa T&S COMP. Tecnología y Servicios S.A.S, para asegurar la Confidencialidad, Integridad, Disponibilidad y control de la información sensible administrada en los procesos de Apoyo, Misionales y Estratégicos, basados en la norma ICONTEC ISO 27001:2013.

3.2 OBJETIVOS ESPECÍFICOS

- Determinar el contexto actual de la empresa T&S COMP. Tecnología y Servicios S.A.S., y las expectativas en relación con el Sistema de Gestión de la Seguridad de la Información.

- Gestionar y clasificar los activos de información de T&S COMP. Tecnología y Servicios S.A.S de los procesos de Apoyo, Misionales y Estratégicos. en materia de Seguridad de la Información.

- Identificar, analizar y valorar los riesgos de Seguridad de la Información asociados a los procesos de Apoyo, Misionales y Estratégicos de la empresa T&S COMP. Tecnología y Servicios S.A.S, basado en la norma ISO 31000:2009.

- Establecer planes de tratamiento de riesgos de Seguridad de la Información para los procesos de Apoyo, Misionales y Estratégicos de la empresa T&S COMP. Tecnología y Servicios S.A.S.

- Definir políticas de Seguridad de la Información para los procesos de Apoyo, Misionales y Estratégicos de la empresa T&S COMP. Tecnología y Servicios S.A.S.

4. MARCO TEÓRICO

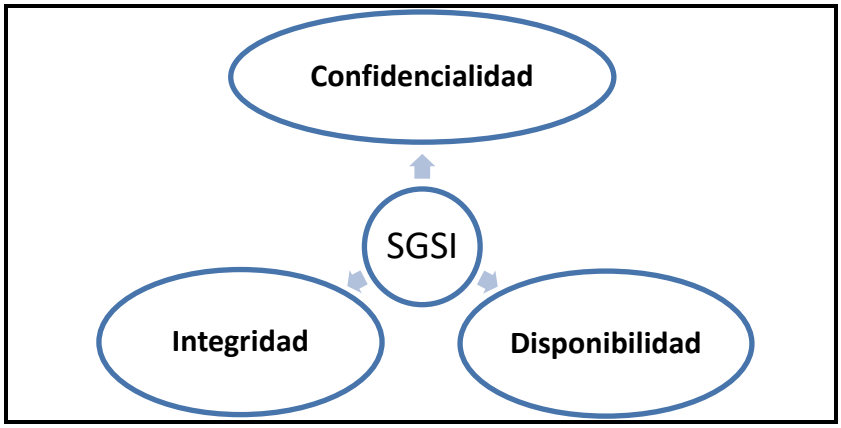
4.1 MARCO REFERENCIAL

4.1.1 Seguridad Informática. La seguridad informática es una estrategia organizacional que tiene como fin principal la protección de las tecnologías de la información y las comunicaciones mediante normas, procedimientos, métodos y técnicas para salvaguardar la información que es generada, almacenada y enviada por sistemas informáticos, bajo los principios de seguridad: Integridad, confidencialidad y disponibilidad. Los sistemas informáticos comprenden: software, hardware, firmware, información y telecomunicaciones.

NIST define la Seguridad Informática como: "*La protección de la información y los sistemas de información contra el acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados a fin de proporcionar confidencialidad, integridad y disponibilidad*."[16]

La *Seguridad de la Información* es un proceso que tiene como propósito principal garantizar los principios fundamentales de seguridad de la información, independientemente de su localización o medio de almacenamiento. Para lograr sus objetivos, la Seguridad de la Información se encuentra fundamentada en tres principios los cuales se muestran en la figura 1:

Figura 1. Principios del SGSI



[16] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Glossary of Key Information Security Terms. [Online]. [Consultado 17 de diciembre de 2016]. Disponible en: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Fuente: Autores[17]

A continuación, se definen los principios de Seguridad de la Información[18]:

- Confidencialidad: Tiene como propósito la privacidad de la información almacenada. Sólo puede estar a disposición de personas o entidades autorizadas para su almacenamiento, modificación y envío.

- Integridad: Consiste en asegurar que la información no sea modificada, alterada, manipulada o borrada sin autorización. Debe ser legítima y consistente con los elementos de información almacenados en el sistema informático por las personas autorizadas. Si ha sido cambiada de manera prohibida, ha perdido su valor original.

- Disponibilidad: Garantizar el acceso a la información procesada en un sistema informático a las personas o entidades autorizadas cuando lo requieran. Debe permitir la continuidad de las actividades en la organización y ser capaz de reestablecerse en caso de falla de manera rápida.

4.1.2 Sistema de Gestión de Seguridad de la Información. El Sistema de Gestión de Seguridad de la Información (o SGSI) es un modelo de seguridad para las empresas que ayuda a generar herramientas para clasificar, evaluar y proteger los activos de información mediante un proceso sistemático y documental.

Debido a que los sistemas de información de las empresas están expuestas a un número elevado de amenazas, el SGSI tiene como beneficios reducir el riesgo de pérdida de información, identificar debilidades del sistema, generar confianza a los clientes y socios, mejorar su imagen, reducir costos, motivación del personal, continuidad de las operaciones del negocio, entre otras.

El modelo del SGSI debe ser suficientemente robusto con procedimientos adecuados para la implementación de controles, en relación con los objetivos del negocio y participación de toda la organización.

Para determinar el Sistema de Gestión de Seguridad de la Información, se utiliza una herramienta con el objetivo de mantener una mejora continua en las organizaciones llamado Ciclo Deming o Ciclo PDCA: Plan (Planificar), Do (Hacer), Check (Verificar) y Act (Actuar)[19] , representado en la figura 2.

[17] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, ISO 27000. [Online]. [Consultado 25 de abril de 2016]. Disponible en: http://www.iso27000.es/download/doc_iso27000_all.pdf
[18] Ibíd.,
[19] INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION, Implementación efectiva de un SGSI ISO 27001. [Consultado el 25 de abril de 2016]. Disponible en:

En la fase de *planificación* se define el alcance del SGSI alineado con los objetivos de la organización, se establece la política general del SGSI, se identifican, analizan y evalúan los riesgos mediante una metodología apropiada, se determinan planes para el tratamiento de riesgos con el objetivo de aplicar controles adecuados, se aprueba por parte de la alta gerencia los riesgos residuales y la implementación del SGSI.

En la fase de *hacer* se implementa el plan de tratamiento de riesgos, controles, métricas para obtener resultados de la eficacia del sistema. Se gestionan los recursos necesarios para el mantenimiento de la seguridad de la información, se determinan controles para la respuesta a incidentes y el desarrollo del marco normativo.[20]

En la fase *verificar* se ejecutan procedimientos de monitorio y revisión para la detección de errores y prevención de incidentes, se verifica la efectividad del SGSI y se realizan auditorías internas, se actualizan planes de seguridad de acuerdo a los resultados encontrados en las auditorías.[21]

Y, por último, en la fase de *actuar* se realizan acciones preventivas y correctivas encontradas en la fase de medición y revisión, se comunican esas mejoras a las partes interesadas y se determina la eficacia de los objetivos del SGSI.[22]

El ciclo PDCA debe ser una herramienta incluida en la estrategia organizacional como un ciclo de vida continuo para todos los procesos dentro de la organización. La aplicación de este método, puede ayudar a que las actividades se realicen de una manera más organizada y eficiente. En la figura 2, se explica gráficamente el proceso del ciclo PDCA del Sistema de Gestión de Seguridad de la Información:

---

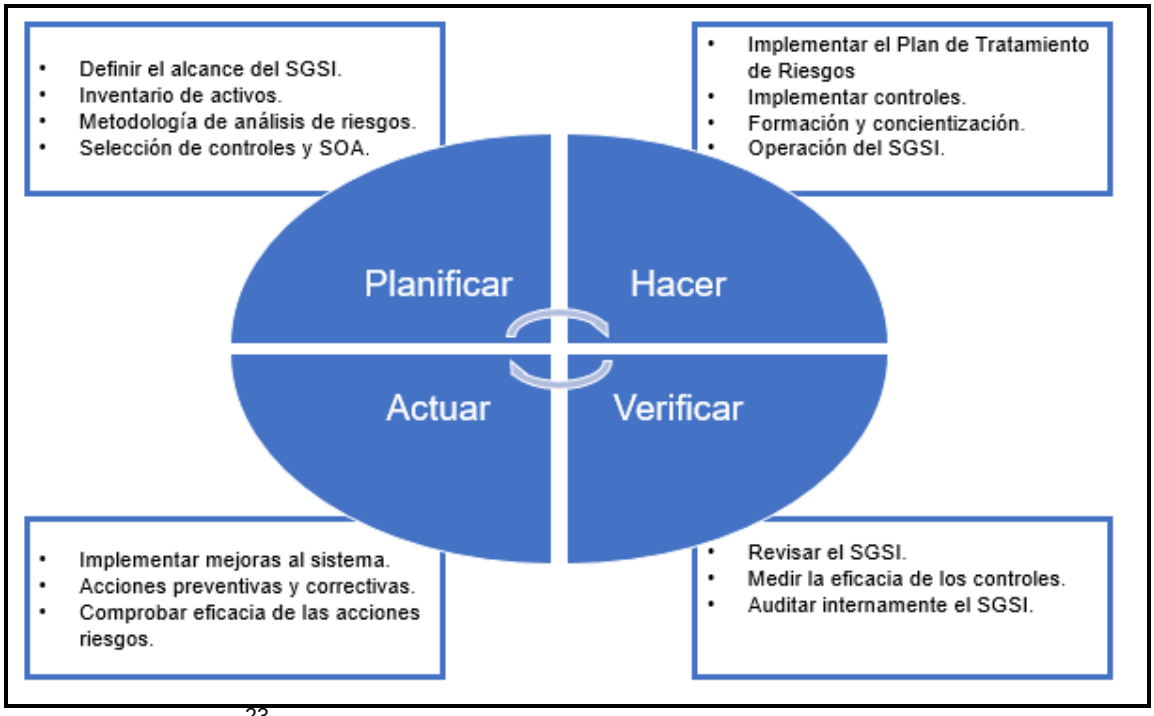
http://www.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2014%20-%20Exposici%C3%B3n%202%20CIGRAS%20ISO%2027001%20-%20rbq.pdf

[20] Ibid,

[21] Ibid,

[22] Ibid,

Figura 2. Ciclo PDCA del SGSI



Fuente: Autores[23]

4.1.3 Normatividad

4.1.3.1 Norma ISO 27001:2013. La Organización Internacional para la Estandarización (ISO) junto con la Comisión Electrotécnica Internacional (IEC, siglas en inglés), suministran los lineamientos para la gestión de la Seguridad de la Información en cualquier tipo de organización. Estas organizaciones publicaron la serie de normas ISO 27000 que contiene especificaciones para las mejores prácticas en las empresas con el fin de desarrollar, implementar y optimizar el Sistema de Seguridad de la Información.[24] Para este proyecto, la norma en la que se enfocará es la ISO 27001:2013.

ISO 27001 es un estándar internacional que tiene como eje central el Sistema de Gestión de Seguridad de la Información. Tiene como objetivo proporcionar

[23] INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION, Implementación efectiva de un SGSI ISO 27001. [Consultado el 25 de abril de 2016]. Disponible en: http://www.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2014%20-%20Exposici%C3%B3n%202%20CIGRAS%20ISO%2027001%20-%20rbq.pdf

[24] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, ISO 27000. [Online]. [Consultado 25 de abril de 2016]. Disponible en: http://www.iso27000.es/download/doc_iso27000_all.pdf

lineamientos para el diseño, implementación, monitoreo, y planes de mejora para el Sistema de Gestión de Seguridad de la Información (SGSI) en la empresa. Se basa en el ciclo PDCA: Plan (Planificar), Do (Hacer), Check (Verificar) y Act (Actuar).

La estructura de la norma ISO 27001:2013 se describe a continuación:

- **Objeto y campo de aplicación:** La norma específica y orienta los requisitos para establecer, implementar, mantener y mejorar el SGSI, así como su uso y finalidad.
- **Referencias normativas:** Relaciona las normas técnicas asociadas para la aplicación de la norma ISO 27001.
- **Términos y definiciones:** Terminología aplicable al estándar.
- **Contexto de la Organización:** En esa etapa se recolecta toda información asociada a la organización, se determinan los aspectos tanto internos como externos para cumplir con los objetivos del negocio, las necesidades y expectativas de las partes interesadas y los aspectos que afectan su capacidad para lograr los objetivos previstos en el SGSI.
- **Liderazgo:** Para el establecimiento de la norma, la alta dirección demuestra su compromiso y liderazgo respecto al SGSI para determinar las políticas y objetivos de seguridad de la información, integrar los requisitos del sistema con los procesos del negocio, apoyar al personal para la adecuada gestión del sistema y promover la mejora continua.
- **Planificación:** De acuerdo a la información recolectada en el apartado del análisis de contexto, se determinan los riesgos asociados al SGSI para establecer objetivos de Seguridad de la Información, tratar los riesgos y prevenir efectos no deseados con el objetivo de lograr una mejora continua.
- **Soporte:** Se disponen y proporcionan los recursos necesarios para el SGSI: competencia, toma de conciencia y comunicación, manteniendo documentado toda la información para la eficacia del sistema.
- **Operación:** Se debe planificar, implementar y controlar los procesos para cumplir con los requisitos previstos en la etapa de planificación, valorar y tratar riesgos conservando la información documentada.
- **Evaluación de desempeño:** En esta etapa se realiza un seguimiento, medición, análisis y evaluación de desempeño del SGSI, con el fin de verificar su funcionalidad y eficacia según lo planeado. Se deben realizar auditorías internas y externas, las cuales deben ser revisadas por la alta dirección para la toma decisiones.
- **Mejora:** Se implementan mejoras propuestas en la etapa de evaluación. Si se reacciona ante una no conformidad se deben tomar acciones y evaluarlas para eliminar las causas y evitar que sucedan. Se mejora continuamente la eficacia del SGSI.

4.1.3.2 Norma ISO 31000:2009. La norma internacional ISO 31000 provee directrices para que las organizaciones gestionen los riesgos con el fin de usar técnicas para identificar y evaluar tanto los riesgos positivos como negativos. El estándar tiene como objetivo ser utilizado por cualquier empresa para ser aplicado en las actividades, estrategias, operaciones, procesos y funciones del día a día.

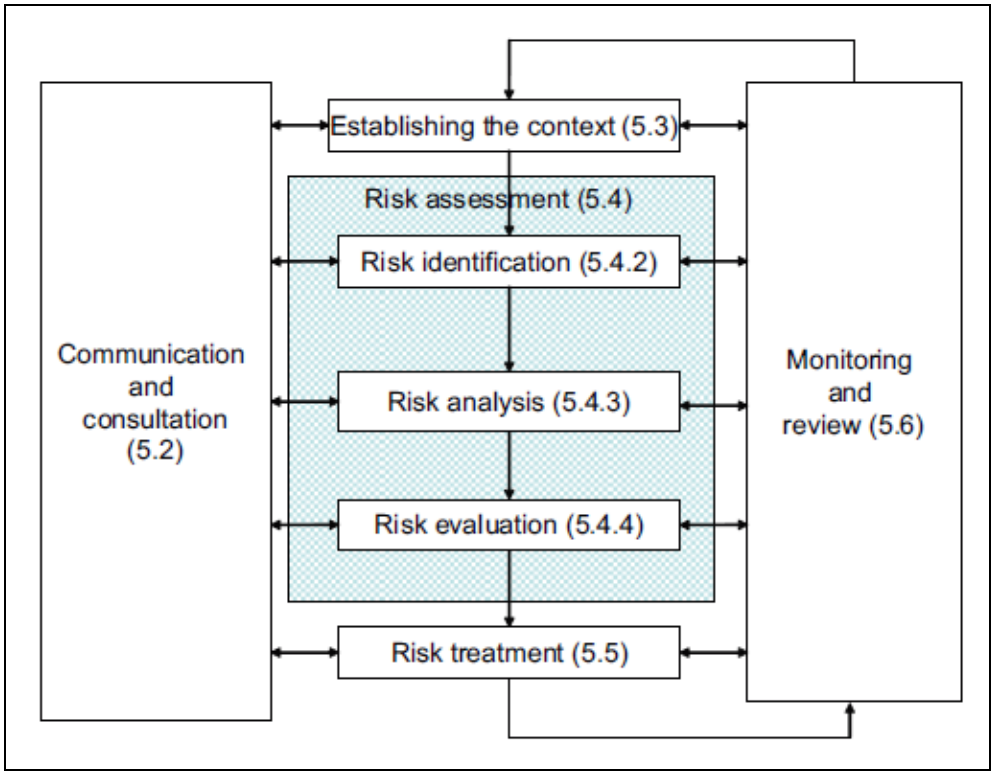
La norma establece principios para que las organizaciones cumplan con una gestión de riesgos eficaz[25]:

a) La gestión de riesgos crea valor y la protege.
b) La gestión de riesgos es parte integral de todos los procesos de la organización.
c) Forma parte de la toma de decisiones.
d) Aborda explícitamente la incertidumbre.
e) Es sistemática, estructurada y oportuna.
f) Se basa en la mejor información disponible.
g) Está adaptado.
h) Integra factores humanos y culturales.
i) Es transparente y participativa.
j) Es dinámica, iterativa y sensible a los cambios.
k) Facilita la mejora continua en la organización.

El proceso de gestión de riesgos, permite a las organizaciones generar sus riesgos con eficiencia e involucrar a los funcionarios a la cultura de mejores prácticas para reducir riesgos y controlar eventos no deseados. La estructura del proceso de gestión de riesgos de la norma ISO 31000:2009, representada en la figura 3, se desarrolla en varias etapas: en la primera etapa se realiza la comunicación y consulta con las partes interesadas tanto internas y externas que se encuentran involucradas en la gestión de riesgos. Seguido de esto, se establecen los contextos internos y externos en cuanto a los riesgos de Seguridad de la Información de la organización de acuerdo a sus objetivos. Como tercera etapa, se realiza la evaluación de riesgos que está conformada por: la identificación, el análisis y evaluación de riesgos de Seguridad de la Información. En la siguiente etapa, se determina el tratamiento de los riesgos identificados en la anterior etapa, para modificarlos e implementar mejoras. Y por último se debe realizar un monitoreo y revisión de manera periódica, con el objetivo de garantizar que los controles sean eficientes.

[25] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO 31000:2009 - Risk management. Principles. Traducido por los autores.

Figura 3. Proceso de evaluación de riesgos ISO 31000:2009



Fuente: International Organization for Standardization [26]

4.2 T&S COMP. TECNOLOGÍA Y SERVICIOS S.A.S

4.2.1 Generalidades de la empresa.

Misión:
"Brindar soluciones de Tecnología Informática, bajo estándares internacionales, apoyados con un equipo calificado y aliados estratégicos, que le permitan a nuestros clientes disponer de una óptima infraestructura tecnológica."[27]

Visión:
"Consolidarnos como centro de servicio autorizado –CSA multifabricante, con presencia a nivel nacional y proyección internacional."[28]

[26] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO 31000:2009 - Risk management. Process. Traducido por los autores.
[27] T&S COMP. TECNOLOGÍA Y SERVICIOS S.A.S. Generalidades de la empresa. [Online] [Consultado el 25 de abril de 2016]. http://tyscomp.com/nosotros/
[28] Ibíd.,

T&S. COMP. Tecnología y Servicios S.A.S., es una entidad privada colombiana, constituida en el año 2001, dedicada a prestar servicios de Tecnologías de la Información y las Comunicaciones. Brindan servicios y productos de calidad avalados con la certificación ISO 9001:2008 y apoyados en las mejores prácticas ITIL. Ofrecen servicio especializado de EPSON Colombia como Centro de Servicio Autorizado EPSON (CSA) para soporte, mantenimiento y reparación de equipos con personal en sitio y con cubrimiento a nivel Nacional.[29]

Para el portafolio de servicios, T&S COMP. Tecnología y Servicios S.A.S cuenta con alta experiencia en mantenimiento preventivo y correctivo para plataformas TI, suministro de partes en líneas de productos EPSON como: Impresoras, LFP, Post Y Video Proyectores y Scanners, venta de equipos, cableado estructurado – Eléctrico y adecuación de Data-Center para dar solución y optimizar la infraestructura tecnológica de acuerdo a las necesidades de sus clientes.

Presenta alianzas estratégicas con empresas como: Microsoft, EPSON, Aranda Software y Dexon Software y algunos de los clientes: Instituto Agropecuario Colombiano (ICA), Armada Nacional de Colombia, Fiscalía General de la Nación, Alcaldía de Usme, entre otras.

T&S COMP. Tecnología y Servicios S.A.S cuenta con 22 empleados, los cuales hacen parte de las áreas de gestión gerencial y de calidad, Servicios y comercial, Facturación, recaudo, compras y almacén, Gestión humana y Sistemas. En el Anexo A, se encuentra el organigrama general de la empresa.[30]

4.2.2. Red de procesos de la empresa. Los procesos con los que cuenta T&S COMP. Tecnología y Servicios S.A.S como base estructural para operar de acuerdo a la gestión de calidad, y representados en la figura 4, son:

- Proceso Estratégico: Encargada de la dirección y el establecimiento de directrices. Dentro de este proceso se encuentran:
- Proceso Gerencial
- Proceso Sistema de Gestión de Calidad (S.G.C)

- Proceso misional: En cargado de la relación directa con los clientes. Se encuentran los siguientes procesos:

- Proceso de Servicios
- Proceso Comercial

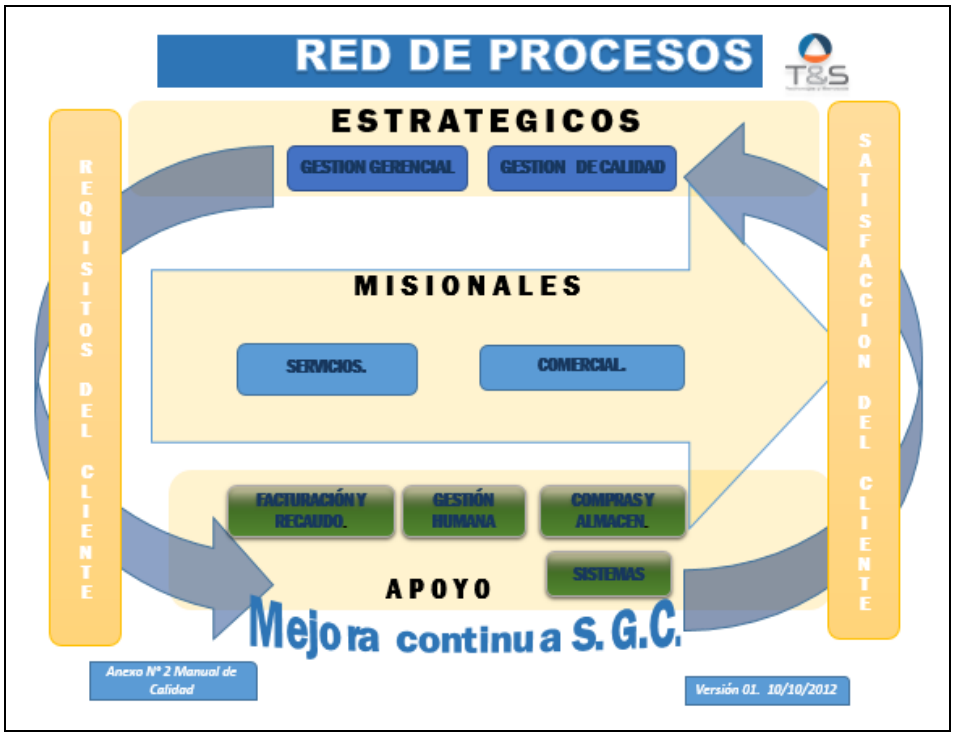
[29] Ibid.
[30] T&S COMP. TECNOLOGÍA Y SERVICIOS S.A.S. Organigrama general. Versión 4. Última actualización: 01/04/2016.

- Procesos de apoyo: Asisten a los procesos misionales para desarrollar sus funciones. Se encuentran:

- Proceso Compras y Almacén
- Proceso Gestión Humana
- Proceso Facturación y Recaudo
- Proceso Sistemas

A continuación, en la figura 4, se muestra la estructura general de la red de procesos de la empresa T&S COMP:

Figura 4. Red de Procesos empresa T&S COMP. Tecnología y Servicios S.A.S



Fuente: T&S COMP. Tecnología y Servicios S.A.S[31]

[31] T&S COMP. TECNOLOGÍA Y SERVICIOS S.A.S. Red de Procesos. Versión 1. Última actualización: 10/10/2012.

4.3 DISEÑO METODOLÓGICO

Para el desarrollo de este proyecto se establecen diferentes actividades para cumplir con los objetivos planteados en el diseño del Sistema de Gestión de Seguridad de la información en la empresa T&S COMP. Tecnología y Servicios S.A.S, basado en la norma ISO 27001:2013. Para este proceso se ejecutan las siguientes etapas:

4.3.1 Etapa 1: Gobierno de la Seguridad. El primer paso para el desarrollo del SGSI en T&S COMP. Tecnología y Servicios S.A.S es establecer el contexto de la organización, identificando el estado actual en cuanto a seguridad de la información por medio de entrevistas y visita a las instalaciones. Se determina el entorno de negocio: procesos que intervienen, estructura organizacional, políticas y procedimientos, clientes y proveedores.

Se identifican sus debilidades y fortalezas frente a la seguridad de la información, para efectuar un análisis de brechas entre el estado actual y el estado deseado de la seguridad de la información en la organización, con el fin de establecer un plan para evitar que ocurran incidentes de seguridad de la información y se generen políticas necesarias para la protección y prevención en el manejo de la información de la organización.

Por otro lado, de acuerdo a la información recolectada en las entrevistas, se analizan las necesidades y expectativas de las partes interesadas, en la cual cada interesado describe cómo se puede satisfacer, y así comprender desde su punto de vista como puede verse afectado en temas de seguridad de la información para establecer planes que cumplan con esas expectativas.

4.3.2 Etapa 2: Planificación de la metodología de riesgos. Se identifican los riesgos por medio de la matriz DOFA y se establecen las fortalezas y las debilidades. Se determinan las amenazas que afectan a la empresa T&S COMP. Tecnología y Servicios S.A.S, para generar la matriz de riesgos y obtener una clasificación de los mismos. A partir de esta matriz, los riesgos son valorados dependiendo el tipo de criticidad de los activos de información para establecer controles que los mitiguen y sean aceptados por la empresa dependiendo el caso. Una vez evaluados, se realiza el plan de tratamiento de riesgos en donde se definen las acciones para mitigar, transferir o aceptar los riesgos identificados. Se genera un documento en donde se registran los controles de seguridad que son aplicables según sea el caso, con el fin de establecer un panorama de los riesgos.

4.3.3 Etapa 3: Tratamiento de riesgos de la seguridad de la información. Una vez valorados los riesgos de seguridad de la información, se establecen planes de

tratamiento en donde se determinan los controles necesarios para obtener por parte de los dueños de los riesgos la aprobación del plan y la aceptación de los riesgos residuales, basados en la ISO 31000.

4.3.4 Etapa 4: Políticas y Alcance del sistema. Se determina primero el alcance del proyecto, es decir, hasta que parte llega el Sistema de Gestión de Seguridad de la Información y cómo la organización se compromete a plantear buenas prácticas para tener una mejora continua.

Se establece la política general de la seguridad de la información en donde se plasma el lineamiento a seguir para el manejo de la información por parte de la organización. Una vez establecida la política, estará disponible para la organización de forma documentada y a su vez estará al alcance de las partes interesadas.

4.3.4.1 Objetivos de seguridad de la información y planes para lograrlos. Se plantean los objetivos de la seguridad de la información, con el objetivo de dar cumplimiento a la política general de seguridad ya definida, los cuales deben ser verificados, aprobados y revisados por la alta gerencia, y además debe estar al alcance de las partes interesadas.

Se establecen los planes para cumplir los objetivos declarando: qué se va a realizar en cada objetivo, qué recursos son necesarios, quiénes son los responsables de hacer cumplir los objetivos, cuándo finaliza y cómo se evalúan los resultados.

4.3.4.2 Roles y responsabilidades en la organización. Se determinan los roles y las responsabilidades que el oficial de la seguridad de la información debe tener frente a la organización, informando a la alta gerencia el desempeño que tenga el sistema de gestión de la seguridad de la información. Así mismo, se establecen los roles y responsabilidades que debe tener todo el personal de la organización.

4.3.4.3 Controles del Sistema de Gestión de la Seguridad de la información. Se realizan controles conforme al tratamiento de los riesgos de la seguridad de la información, de acuerdo al anexo A de la norma ISO 27001:2013.

4.3.5 Etapa 5: Soporte. Se proporcionan los recursos necesarios para el establecimiento, implementación y mejora continua del sistema de gestión de la seguridad de la información.

4.3.5.1 Plan de toma de conciencia. Se realizan charlas a la alta dirección y a los empleados, en donde se divulga la política de seguridad de la información que se estableció para la empresa T&S COMP. Tecnología y Servicios S.A.S. Para el plan de toma de conciencia se explica qué beneficios trae la gestión de la seguridad de la información a la empresa, cómo se debe cumplir con los lineamientos de la seguridad para hacer efectivo el Sistema de Gestión de Seguridad de la Información, haciendo uso de buenas prácticas en cada proceso.

4.3.5.2 Comunicación. La empresa T&S COMP. Tecnología y Servicios S.A.S, realizara las comunicaciones por intermedio de la gerente general y el coordinador TI , ya sea por correo electrónico o de forma escrita, siempre y cuando se deba notificar: Cumplimiento de las políticas y sus modificaciones, la ocurrencia de algún evento que comprometa la seguridad de la información en sus pilares, integridad, confidencialidad y disponibilidad, cambios en las políticas de la seguridad de la información, en general a todos los empleados que estén involucrados en cada proceso de la empresa.

5. CONTEXTO DE LA SEGURIDAD DE LA INFORMACIÓN EN T&S COMP. TECNOLOGÍA Y SERVICIOS S.A.S.

Con el continuo cambio que van presentado las tecnologías de la información y las comunicaciones, se requiere una dinámica constante para salvaguardar la información por el gran valor que constituyen en las organizaciones. Sin embargo, las PYME están más expuestas a ciberataques ya sea por su inexperiencia o por falta de estructuras de seguridad de la información. Por esta razón, las entidades de prestación de servicios tecnológicos se ven en la necesidad de establecer, gestionar e implementar de manera correcta el Sistema de Gestión de Seguridad de la Información (SGSI), preservando la confidencialidad, integridad y disponibilidad de su información.

Para establecer la integridad, disponibilidad y confidencialidad de la información en un modelo de negocio orientado a la prestación de servicios tecnológicos, se deben adoptar procesos adecuados para la planeación, implementación, mantenimiento y mejora del SGSI, de acuerdo a la norma ISO 27001:2013.

Para efectos del diseño del SGSI en la empresa T&S COMP. Tecnología y Servicios S.A.S, se desarrollarán las siguientes etapas para preservar los principios de Seguridad de la Información en la organización: Determinar el contexto y estado actual de la entidad, gestionar y clasificar activos de información, identificar, analizar y valorar los riesgos en cuanto a la Seguridad de la Información, establecer planes de tratamiento de los riesgos y definir políticas y controles de Seguridad de la Información.

La primera etapa, tiene como objetivo el análisis y conocimiento de la organización para determinar que amenazas los afectan tanto interna como externamente, identificar los recursos a proteger y establecer el nivel de riesgo al cual están expuestos los procesos de Apoyo, Misionales y Estratégicos.

5.1 ESTADO ACTUAL DE T&S COMP. TECNOLOGÍA Y SERVICIOS S.A.S.

T&S COMP. Tecnología y Servicios S.A.S. es una empresa colombiana encargada de prestar servicios tecnológicos como Centro de Servicio Autorizado EPSON (CSA) para brindar reparación y soporte de equipos. Son mayoristas de partes EPSON y ofrecen soluciones en gestión de infraestructura informática junto con Aranda Software. En su interés por asegurar su información, T&S COMP. Tecnología y Servicios S.A.S, orienta sus esfuerzos para la consecución y desarrollo de este proyecto, para ser implementado dentro de su entorno de seguridad.

Para el diseño del SGSI en los procesos de la empresa, basado en la norma ISO 27001:2013, se establecen dos tipos de factores para el análisis de amenazas: internos y externos. Para determinar los factores internos, inicialmente se hace un reconocimiento de la organización como: su objetivo principal, estructura organizacional, procesos y subprocesos, expectativas y percepciones de los involucrados internos, identificación de activos y sistemas de información. Por otro lado, se identifican los externos como: Partes involucradas externas (clientes, proveedores), factores medioambientales y tecnológicos, el ambiente económico, político y social.

A partir de estos factores se identifican las amenazas que intervienen, afectando la seguridad de su información que da como resultado una infraestructura tecnológica vulnerada. Un error que generalmente ocurre en la entidad es la inadecuada gestión de conocimiento sobre el valor que tiene la información y por tanto no fortalecen su sistema de seguridad para salvaguardar sus activos.

En la figura 5, se describen las debilidades más comunes que se presentan en T&S COMP. Tecnología y Servicios S.A.S:

Figura 5. Debilidades comunes de T&S COMP. Tecnología y Servicios S.A.S.

Fuente: Autores, Información suministrada por T&S COMP.

De acuerdo a las debilidades descritas en la figura 5, en T&S COMP. Tecnología y Servicios S.A.S se evidencian debilidades que serán tratadas empleando el Sistema de Gestión de Seguridad de la Información y orientándose a la búsqueda de la protección de los activos de información en la organización. Para el enfoque de este proyecto en T&S COMP. Tecnología y Servicios S.A.S, se determinarán procesos que ayuden a reducir posibles amenazas que afecten sus recursos valiosos, evitando que la información confidencial pase a manos de personas mal intencionadas, formando a sus trabajadores en seguridad de la información y fortaleciendo sus sistemas tecnológicos para que disfrute de un ambiente estable y seguro.

5.1.1 Matriz DOFA. Permite enfrentar la diversidad de factores internos (fortalezas y debilidades) y externos (oportunidades y amenazas) en los procesos de Apoyo, Misionales y Estratégicos de la empresa T&S COMP. Tecnología y Servicios S.A.S, generando alternativas y estrategias para mejorar la gestión de TIC enfocadas en la seguridad informática, como se evidencia en el cuadro 1.

Cuadro 1. Matriz DOFA T&S COMP. Tecnología y servicios S.A.S

	Debilidades (D)	**Fortalezas (F)**
Matriz DOFA Contexto Interno	1.Desconocimiento de activos vitales e información confidencial de cada proceso de T&S COMP. Tecnología y Servicios S.A.S. 2. Ausencia de un gobierno de la seguridad de la información en la empresa T&S COMP. Tecnología y Servicios S.A.S. 3. Desactualización e inadecuada clasificación del inventario de los activos de información. 4. Desconocimiento de los riesgos asociados al incorrecto manejo de la información, por parte de los empleados. 5. Ausencia de procesos y controles para el manejo de la información personal. 6. Inexistencia de procesos definidos para realizar escaneo de vulnerabilidades. 7. Ausencia de aseguramiento de la página web.	1. Participación por parte de la alta gerencia en la implementación de un Gobierno de Seguridad de la Información en la empresa. 2. Revisión de antecedentes en el proceso de contratación de personal ante las autoridades pertinentes. 3. Inclusión de cláusulas de confidencialidad de la información en los contratos con entidades estatales (clientes). 4. Servidor de réplica en tiempo real para realizar Backups de toda la información de la compañía y almacenamiento semanal en discos encriptados. 5. Plan de contingencia para almacenar en la nube los datos generados en el árbol de información de la empresa. 6. Adquisición de CCTV y monitoreo constante para la supervisión física al interior y exterior de la empresa

Cuadro 1. (Continuación)

Matriz DOFA Contexto interno	**Debilidades (D)**	**Fortalezas (F)**
	8. Falta de compromiso por parte del personal de T&S COMP. Tecnología y Servicios S.A.S sobre la importancia de la seguridad de la información en las labores diarias. 9. Ausencia de control de acceso a las instalaciones de la compañía. 10. Inexistencia de planes para la gestión de continuidad de negocio.	7. Contratación de proveedor de Servicios de Internet de respaldo, en caso que falle el actual. 8. Adquisición de UPS (Uninterruptible Power Supply) para apagado correcto de los equipos en caso que se presente suspensión inesperada de energía eléctrica. 9. Bloqueo de Puertos USB para evitar fuga de información. 10. Adquisición de antivirus para el aseguramiento de la información. 11. Gestión documental para digitalizar los documentos físicos de la compañía. 12. Acceso restringido al Centro de Datos por medio de Sistema Biométrico.
Oportunidades (O) Contexto Externo	**Estrategias (DO)**	**Estrategias (FO)**
	1. Establecer un Gobierno de seguridad de la información y los respectivos lineamientos de seguridad para proteger los recursos de la compañía.	1. Implementación de un gobierno de seguridad de la información con la ayuda de la Alta Gerencia.

Cuadro 1. (Continuación)

Oportunidades (O) Contexto Externo	**Estrategias (DO)**	**Estrategias (FO)**
1. Generación de confianza por parte de nuevos clientes. 2. Implementación de buenas prácticas de seguridad de la información, para diferenciarse de la competencia. 3. Consecución de nuevos clientes e incremento de procesos licitatorios. 4. Implementación de nuevos controles para el manejo de la información personal, de acuerdo con las normas de protección de datos personales.	2. Realizar actualización del inventario de activos de información cada año con el apoyo de todas las áreas, por medio de capacitaciones para saber cuáles son los activos vitales de la compañía. 3. Realizar campañas de concientización al personal de T&S COMP. Tecnología y Servicios S.A.S sobre la importancia de la seguridad de la información en el desarrollo de cada labor. 4. Determinar y divulgar las políticas de seguridad informática de acuerdo con el estándar ISO 27001, a todas las partes interesadas. 5. Implementar controles para el manejo de la información personal basado en la ley de protección de datos personales.	2. Consolidar el proceso de contratación de personal, por medio de cláusulas que brinden confidencialidad de la información, para adquirir nuevos clientes. 3. Fomentar buenas prácticas para evitar el acceso a sitios web no autorizados. 4. Realizar mantenimientos preventivos a la UPS, para garantizar su buen funcionamiento. 5. Realizar capacitaciones en seguridad de la información a los empleados de la organización para evitar fuga de información. 6.Consolidar los controles de acceso a las instalaciones, para generar confianza a nuevos clientes.

Cuadro 1. (Continuación)

Oportunidades (O) Contexto Externo	**Estrategias (DO)**	**Estrategias (FO)**
	6. Implementar controles y planes de mejora para asegurar el ingreso de personal externo a las instalaciones de la compañía, para salvaguardar los activos de información. 7. Acompañar a todas las áreas para identificar todos los riesgos de seguridad de la información, para la creación de planes de continuad del negocio.	7. Fortalecer controles para salvaguardar la información digitalizada de la compañía, por medio de buenas prácticas. 8. Reforzar controles de seguridad para el acceso al Datacenter en caso de falla del Sistema Biométrico, para garantizar la continuidad del negocio.
Amenazas (A) Contexto Externo	**Estrategias (DA)**	**Estrategias (FA)**
	1. Establecer el Gobierno de seguridad informática para la administración y gestión de los recursos, y generar medidas necesarias para salvaguardar la información de amenazas que puedan afectar el correcto desarrollo de las actividades de la compañía. 2. Ejecutar la actualización continua del inventario de los activos de información para evitar pérdidas, alteración o acceso no autorizado a datos confidenciales.	1. Implementación de un gobierno de seguridad para reducir y mitigar amenazas asociados a la pérdida de integridad, confidencialidad y disponibilidad de la información. 2. Reforzar estrategias de concientización a todo el personal, para generar cultura de seguridad de la información y poder competir con la competencia y adquirir una ventaja.

Cuadro 1. (Continuación)

Amenazas (A) **Contexto Externo** 1. Fallas en el servicio de energía, o proveedor de servicio de red. 2. Perdida o alteración de la información. 3. Fenómenos naturales. 4. Empresas que presten este mismo servicio, pero con estructura organizacional más sólida y competitiva. 5. Inobservancia a las disposiciones de la ley de protección de datos personales.	**Estrategias (DA)**	**Estrategias (FA)**
	3. Fortalecer el plan de continuidad del negocio para garantizar las líneas de negocio, ante cualquier desastre. 4. Realizar seguimiento al funcionamiento de la UPS por medio de mantenimientos preventivos, por medio de una empresa especializada cada 6 meses. 5. Mantener actualizado el antivirus, para impedir que los equipos sean vulnerados, exista perdida o alteración de la información. 6. Realizar la digitalización de la información física en el menor tiempo posible, para evitar que pierda su disponibilidad por fenómenos naturales. 7. Monitorear al ingreso no autorizado al Datacenter, para evitar comprometer la información vital de la compañía y sea alterada por un externo a la empresa.	3. Identificar los activos vitales de la empresa para ser protegidos ante amenazas a las que pueden estar expuestos. 4. Realizar campañas de concientización al personal de T&S COMP. Tecnología y Servicios S.A.S sobre la importancia de la seguridad de la información. 5. Implementar controles para el manejo de la información personal basado en la ley de protección de datos personales para evitar el procesamiento ilegal de la información personal que se maneja en la organización. 6. Realizar mensualmente un escaneo de vulnerabilidades para identificarlas y eliminarlas, e impedir que sea comprometida la seguridad del sistema de información de la compañía. 7. Asegurar la página web para evitar que atacantes generen Denegación de Servicio y se vea afectada la imagen de la empresa.

Cuadro 1. (Continuación)

Amenazas (A) **Contexto Externo**	**Estrategias (DA)**	**Estrategias (FA)**
	8. Realizar planes de mejora y controles para asegurar el ingreso de personal externo para prevenir el acceso no autorizado a las instalaciones de la compañía. 9. Cumplir con todas las disposiciones legales referentes a la protección de datos personales y capacitar a todo el personal de la empresa para que aplique las leyes y le eviten multas a la empresa.	8. Realizar monitoreo continuo de la seguridad física en caso de pérdida de suministro de energía y contar con un plan de contingencia. 9. Revisar constantemente los cambios en la estructura organizacional, para hacer extensiva la información a todos los colaboradores.

Fuente: Autores. Información suministrada por T&S COMP.

Una vez realizado el análisis de la situación actual de la empresa T&S COMP. Tecnología y Servicios S.A.S, se obtuvieron los siguientes resultados en el cuadro 2, en base a los objetivos de Sistema de Gestión de Seguridad de la Información:

Cuadro 2. Estrategias DOFA T&S COMP. Tecnología y Servicios S.A.S

Objetivos SGSI	Estrategias
DO Cumplir con los principios y ser coherentes con la política de seguridad de la información en la empresa T&S COMP. Tecnología y Servicios S.A.S	1. Establecer un Gobierno de seguridad de la información y los respectivos lineamientos de seguridad para proteger los recursos de la compañía. 2. Realizar actualización del inventario de activos de información cada año con el apoyo de todas las áreas, por medio de capacitaciones para saber cuáles son los activos vitales de la compañía. 3. Realizar campañas de concientización al personal de T&S COMP. Tecnología y Servicios S.A.S sobre la importancia de la seguridad de la información en el desarrollo de cada labor. 4. Determinar y divulgar las políticas de seguridad informática de acuerdo con el estándar ISO 27001, a todas las partes interesadas. 5. Implementar controles para el manejo de la información personal basado en la ley de protección de datos personales. 6. Implementar controles y planes de mejora para asegurar el ingreso de personal externo a las instalaciones de la compañía, para salvaguardar los activos de información. 7. Acompañar a todas las áreas para identificar todos los riesgos de seguridad de la información, para la creación de planes de continuad del negocio.

Cuadro 2. (Continuación)

Objetivos SGSI	Estrategias
DA Mejorar y realizar acciones preventivas y correctivas para el Sistema de Gestión de Seguridad de la Información.	1. Establecer el Gobierno de seguridad informática para la administración y gestión de los recursos, y generar medidas necesarias para salvaguardar la información de amenazas que puedan afectar el correcto desarrollo de las actividades de la compañía. 2. Ejecutar la actualización continua del inventario de los activos de información para evitar pérdidas, alteración o acceso no autorizado a datos confidenciales. 3. Fortalecer el plan de continuidad del negocio para garantizar las líneas de negocio, ante cualquier desastre. 4. Realizar seguimiento al funcionamiento de la UPS por medio de mantenimientos preventivos, por medio de una empresa especializada cada 6 meses. 5. Mantener actualizado el antivirus, para impedir que los equipos sean vulnerados, exista perdida o alteración de la información. 6. Realizar la digitalización de la información física en el menor tiempo posible, para evitar que pierda su disponibilidad por fenómenos naturales. 7. Monitorear al ingreso no autorizado al Datacenter, para evitar comprometer la información vital de la compañía y sea alterada por un externo a la empresa. 8. Realizar planes de mejora y controles para asegurar el ingreso de personal externo para prevenir el acceso no autorizado a las instalaciones de la compañía. 9. Cumplir con todas las disposiciones legales referentes a la protección de datos personales y capacitar a todo el personal de la empresa para que aplique las leyes y le eviten multas a la empresa.

Cuadro 2. (Continuación)

Objetivos SGSI	Estrategias
FO Incentivar mejores prácticas a todos los empleados, por medio de jornadas de concientización.	1. Implementación de un gobierno de seguridad de la información con la ayuda de la Alta Gerencia. 2. Consolidar el proceso de contratación de personal, por medio de cláusulas que brinden confidencialidad de la información, para adquirir nuevos clientes. 3. Fomentar buenas prácticas para evitar el acceso a sitios web no autorizados. 4. Realizar mantenimientos preventivos a la UPS, para garantizar su buen funcionamiento. 5. Realizar capacitaciones en seguridad de la información a los empleados de la organización para evitar fuga de información. 6.Consolidar los controles de acceso a las instalaciones, para generar confianza a nuevos clientes. 7. Fortalecer controles para salvaguardar la información digitalizada de la compañía, por medio de buenas prácticas. 8. Reforzar controles de seguridad para el acceso al Datacenter en caso de falla del Sistema Biométrico, para garantizar la continuidad del negocio.
FA Implementar controles para mantener actualizados los activos vitales de la empresa y el plan de contingencia, garantizando la continuidad de la información.	1. Implementación de un gobierno de seguridad para reducir y mitigar amenazas asociados a la pérdida de integridad, confidencialidad y disponibilidad de la información. 2. Reforzar estrategias de concientización a todo el personal, para generar cultura de seguridad de la información y poder competir con la competencia y adquirir una ventaja. 3. Identificar los activos vitales de la empresa para ser protegidos ante amenazas a las que pueden estar expuestos.

Cuadro 2. (Continuación)

Objetivos SGSI	Estrategias
FA Implementar controles para mantener actualizados los activos vitales de la empresa y el plan de contingencia, garantizando la continuidad de negocio frente a incidentes.	4. Realizar campañas de concientización al personal de T&S COMP. Tecnología y Servicios S.A.S sobre la importancia de la seguridad de la información. 5. Implementar controles para el manejo de la información personal basado en la ley de protección de datos personales para evitar el procesamiento ilegal de la información personal que se maneja en la organización. 6. Realizar mensualmente un escaneo de vulnerabilidades para identificarlas y eliminarlas, e impedir que sea comprometida la seguridad del sistema de información de la compañía. 7. Asegurar la página web para evitar que atacantes generen Denegación de Servicio y se vea afectada la imagen de la empresa. 8. Realizar monitoreo continuo de la seguridad física en caso de pérdida de suministro de energía y contar con un plan de contingencia. 9. Revisar constantemente los cambios en la estructura organizacional, para hacer extensiva la información a todos los colaboradores.
Fuente: Autores. Información obtenida de la matriz DOFA.	

5.1.2 Análisis de brecha. Una vez analizada la situación actual de la empresa referente a la Seguridad de la información, identificando cuáles son sus debilidades y fortalezas se determinó lo siguiente de acuerdo a los controles del anexo A de la norma ISO 27001:2013, en el cuadro 3 se explica la clasificación de cumplimiento, que se aplica para el análisis de brechas por dominio de control.

Cuadro 3. Clasificación de cumplimiento

Estado	Significado
Cumple satisfactoriamente	Existe, es gestionado, se está cumpliendo con lo que la norma solicita, está documentado, es conocido y aplicado por todos los involucrados en el SGSI cumple 100%.
Cumple parcialmente	Lo que la norma requiere se está haciendo de manera parcial, se está haciendo diferente, no está documentado, se definió, pero no se gestiona.
No cumple	No existe y/o no se está haciendo.
No aplica	El control no es aplicable para la entidad. En el campo evidencia por favor indicar la justificación respectiva de su no aplicabilidad.

Fuente: ALTA CONSEJERIA DISTRITAL DE TIC [32]

[32] ALTA CONSEJERIA DISTRITAL DE TIC. Autodiagnóstico SGSI V2 [Online]. [Consultado 16 de enero de 2017]. Disponible en: tic.bogota.gov.co/sites/default/files/.../AutodiagnosticoSGSI_v2_09072015.xls

Tabla 1. Análisis de Brecha por Dominio de Control

Por dominio de control						
Nombre dominios de control	**Controles que aplican**	**Peso controles implementados y parcialmente implementados**	**Implementados**	**Parcialmente**	**No cumple**	**No aplica**
Dominio 5 - políticas de seguridad de la información	2	0	0	0	2	0
Dominio 6 - organización de la seguridad de la información	6	2	0	4	2	1
Dominio 7 - seguridad de los recursos humanos	6	3,5	1	5	0	0
Dominio 8 - gestión de activos	10	5	2	2	6	0
Dominio 9 - control de acceso	14	9	6	2	6	0
Dominio 10 – criptografía	2	1,5	1	1	0	0
Dominio 11 - seguridad física y del entorno	15	9	5	8	2	0
Dominio 12 - seguridad de las operaciones	14	6,5	2	9	3	0

Tabla 1. (Continuación)

Por dominio de control						
Nombre dominios de control	**Controles que aplican**	**Peso controles implementados y parcialmente implementados**	**Implementados**	**Parcialmente**	**No cumple**	**No aplica**
Dominio 13 - seguridad de las comunicaciones	7	4	2	4	1	0
Dominio 14 - adquisición, desarrollo y mantenimiento de sistemas	6	2	0	4	2	7
Dominio 15 - relación con los proveedores	5	2	1	2	2	0
Dominio 16 - gestión de incidentes de seguridad de la información	7	2,5	0	5	2	0
Dominio 17 - aspectos de seguridad de la información de la gestión de continuidad de negocio	4	2,5	1	3	0	0
Dominio 18 – cumplimiento	8	2,5	1	3	4	0
Total	106					

Fuente: ALTA CONSEJERIA DISTRITAL DE TIC[33]

[33] Ibíd.

Los datos anteriores fueron extraídos de acuerdo a los 18 dominios de control del Anexo A de la Norma ISO 27001:2013. Por cada dominio se determinó qué controles aplican y cuáles de estos se cumplen parcial o satisfactoriamente, cuáles no se cumplen o no aplican según el tipo de actividad de la empresa, enfocándose en los controles que no cumplen, realizando un monitoreo de lo que se está implementando con el fin de dar cumplimiento a la norma, como se evidencia en la tabla 1.

Teniendo en cuenta la información anterior, se determinó que existen falencias principalmente en los controles de políticas de seguridad de la información, Gestión de activos, Control de Acceso y cumplimiento de las políticas de seguridad, para lo cual se realizan las siguientes recomendaciones:

Dominio 1. Políticas de Seguridad de la Información: Se recomiendo la implementación de políticas de seguridad, para que sean aplicables a todos los procesos de la empresa y entren en conocimiento de todos los empleados de la misma, y a su vez sean aprobadas por la alta gerencia, también se debe llevar un control en caso de que se realicen cambios significativos, para garantizar su adecuación y eficacia continua.

Dominio 8. Gestión de Activos: Se realizó la identificación de los activos en el que se registraron en un inventario en colaboración de cada una de las áreas implicadas en los procesos de la empresa. Se deben identificar los activos vitales de la compañía y establecer controles para el manejo de los mismos y mantener actualizado el inventario de activos.

Dominio 9. Control de Acceso: Se recomendó establecer mejores procedimientos para el control de acceso a las instalaciones teniendo en cuenta que no tienen procesos adecuados. Se debe monitorear los accesos a la red por parte de los empleados y sus privilegios según corresponda el perfil de usuario.

Dominio 18. Cumplimiento: Se propuso implementar procedimientos adecuados para el cumplimiento de las políticas de seguridad, y los requisitos legislativos una vez sean implementados en la empresa, se controlar periódicamente el estricto cumplimiento de las mismas por todo el personal.

5.1.3 Comprensión de necesidades. Se establece por medio de una encuesta a los interesados internos y externos, (Anexo B), las expectativas y necesidades respecto a la seguridad de la información y la forma de satisfacer esas necesidades que se generan en cada uno de los procesos de la empresa T&S COMP. Tecnología y Servicios S.A.S. En el cuadro 4 se observan los resultados obtenidos:

Cuadro 4. Análisis de interesados

Tipo de interesado	Interesado	Expectativa	Necesidad	Forma de satisfacer la necesidad
Interno	Gerencia	Poder salvaguardar la información vital de la empresa, por medio de buenas prácticas de seguridad de la información.	Salvaguardar la información vital de la empresa.	Implementar un Sistema de Gestión de Seguridad de la Información.
Interno	Coordinador IT	Mantener un control constante sobre la seguridad de la información.	Establecer los procedimientos para el control constante sobre la seguridad de la información.	Concientización a los líderes de procesos sobre la importancia y peligros que se deben tener en cuenta en el manejo de la información del día a día.
Interno	Coordinadora de licitaciones	Teniendo en cuenta la naturaleza de la información, debe existir una seguridad que garantice que los archivos no sean alterados.	Establecer controles para que el acceso a la información solo sea a través de las personas que intervienen en el proceso.	Por medio de políticas de seguridad en donde se impongan controles para el acceso a la información.
Interno	Jefe de compras	Seguridad de la información de los proveedores y los Backorders.	Salvaguardar la información de los proveedores y Backorders.	Bloquear la información al personal no autorizado.

Cuadro 4. (Continuación)

Tipo de interesado	Interesado	Expectativa	Necesidad	Forma de satisfacer la necesidad
Interno	Tesorero y control interno	Confidencialidad en la información manejada.	Evitar que la información de la empresa sea divulgada.	Restringir el acceso al personal no autorizado.
Interno	Colaboradores	Resguardar la información de los clientes, en temas de cobros de servicios realizados.	Garantizar la integridad de la información de los clientes.	Mayor control de los perfiles de los usuarios, para garantizar la integridad de la información, además se debe realizar Backups en caso de caída del sistema.
Externo	Proveedores	Prolongación en la contratación, cumplimiento en pagos y protección de la información personal.	Evitar que la información suministrada por los proveedores sea divulgada.	Establecer controles con cada uno de los contratos que se establezcan con los proveedores, garantizando la confidencialidad de la información suministrada.
Externo	Clientes	Protección de la operación para que le aseguren servicio seguro, así como su información personal.	Proteger los datos personales, deben ser confidenciales.	Estricto cumplimiento de las leyes de protección y manejo de los datos personales, garantizando la confidencialidad de la información suministrada.

Fuente: Autores. Entrevistas realizadas a las partes interesados (Anexo B).

Teniendo en cuenta la información obtenida en el cuadro 4, los interesados plasmaron sus expectativas y necesidades respecto a la seguridad de la información en la empresa T&S COMP. Tecnología y Servicios S.A.S. Se determinó que varios de los interesados tienen puntos en común para poder satisfacer esas necesidades como las buenas prácticas para el manejo de la información de la empresa y establecer procedimientos para salvaguardar la información tanto a nivel interno como externo.

Los interesados hicieron énfasis en establecer controles para clientes y proveedores con el fin de evitar pérdida de información, garantizar su integridad y brindar confidencialidad tanto para la empresa como para los clientes y proveedores.

De la misma manera, por medio de políticas de la seguridad de la información se pueden establecer requisitos, para mantener y mejorar el SGSI que los interesados están solicitando, para satisfacer sus expectativas como parte integral de la empresa.

A nivel de requisitos legales, se puede encontrar la Ley de protección de datos personales Ley 1581 de 2012, en donde "**Artículo 1°. Objeto.** La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma[34]", tanto clientes como proveedores suministran información sensible que no debe ser divulgada , debe ser manejada y administrada por la empresa y para la empresa, garantizando ese derecho de protección a su información, teniendo en cuenta que las leyes son de obligatorio cumplimiento.

[34] ALCALDÍA MAYOR DE BOGOTÁ. Ley Estatutaria 1581 DE 2012 [Online]. [Consultado 20 de diciembre de 2016]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

6. GESTIÓN Y CLASIFICACIÓN DE ACTIVOS T&S COMP. TECNOLOGÍA Y SERVICIOS S.A.S

Los activos son el corazón y la parte fundamental para el pleno desarrollo de las actividades de las empresas, por esto, con una administración efectiva de cada uno de sus recursos se logra un conocimiento de lo que se tiene y una distribución eficaz, adecuada y organizada en el momento que se requiera. El objetivo de los inventarios de activos, es identificar y controlar de forma precisa los recursos existentes en la organización. Por esta razón, en este capítulo se determinará la gestión y clasificación de los activos en los procesos de Apoyo, Misionales y Estratégicos de T&S COMP. Tecnología y Servicios S.A.S para establecer la integridad, disponibilidad y confidencialidad de la información en un modelo de negocio orientado a la prestación de servicios tecnológicos.

Esta etapa del SGSI, consiste en identificar y evaluar la importancia de los activos críticos de T&S COMP. Tecnología y Servicios S.A.S., en el que se valorarán en una escala para definir su relevancia en las actividades de la empresa y cumplir con los objetivos del negocio. Una vez identificado el valor de los recursos, se dará paso al análisis de riesgo.

6.1 IDENTIFICACIÓN DE ACTIVOS DE T&S COMP. TECNOLOGÍA Y SERVICIOS S.A.S.

Las actividades para la clasificación de activos son: identificación, revisión, actualización y publicación; en términos del diseño del sistema, se realizará la identificación de los activos con ayuda de los líderes de los procesos de Apoyo, Misionales y Estratégicos. Para identificar los activos, se registrarán en el inventario con información de las características de cada uno de los recursos:

- **Identificador:** Número de identificación del activo.
- **Proceso:** Proceso al que pertenece el activo.
- **Nombre del Activo:** Nombre del activo de información de acuerdo al proceso al que pertenece.
- **Descripción/Observaciones:** Detalle del activo de forma que sea fácilmente identificable por los miembros del proceso.

- **Tipo**:

- Información: Tipo de datos que son almacenados física o electrónicamente (archivos, bases de datos, manuales, contratos, auditorías, entre otros)
- Recurso Humano: Personas que por su conocimiento y experiencia son considerados activos.
- Software: Interfaces, software de los sistemas, aplicaciones de desarrollo, entre otros.
- Servicio: Servicios como páginas de Internet, páginas de consulta, intranet, entre otros.
- Hardware: Equipos de cómputo que dependiendo a la información que almacenan son considerados críticos.
- Instalaciones: Lugares donde se encuentran los sistemas de información y activos críticos de la entidad.

- **Ubicación**: Ubicación física o electrónica donde se encuentra el activo de información.

- **Propietario**: Funcionario que tiene a cargo el activo de información. Tiene la responsabilidad de garantizar que los activos de información estén clasificados correctamente.

En el cuadro 5, se presenta el inventario de activos T&S COMP. Tecnología y Servicios S.A.S., generado en conjunto con los líderes de los procesos:

Cuadro 5. Inventario de Activos T&S COMP. Tecnología y Servicios S.A.S.

ID	Proceso	Nombre del Activo	Tipo	Ubicación	Propietario	Descripción	Gestión	
							Fecha de Ingreso	Fecha de Salida
1	Misional / Servicios	Informe mensual gerencia.	Información	Servidor file server/documentos/3-actividades\entrega informe	Alejandra Barragán	Formato presentación de informe a gerencia f506.04.	11/03/2016	N/A
2	Misional / Servicios	Indicadores administrativa y servicio	Información	Servidor file server/documentos/3-actividades\entrega informe	Alejandra Barragán	Indicadores administrativa y servicios.	11/03/2016	N/A
3	Misional / Servicios	Localización archivo físico administrativa y servicios	Información	Servidor file server/documentos/4-ubicacion archivo físico	Alejandra Barragán	Registro donde se describe la ubicación y contenido del archivo físico de administrativa y servicios.	20/01/2014	N/A
4	Misional / Servicios	Ubicación general archivo físico general de la empresa	Información	Servidor file server/documentos/4-ubicacion archivo físico	Alejandra Barragán	Registro donde se describe la ubicación y contenido del archivo físico general de la empresa.	3/02/2014	23/12/2015

Cuadro 5. (Continuación)

ID	Proceso	Nombre del Activo	Tipo	Ubicación	Propietario	Descripción	Gestión	
							Fecha de Ingreso	Fecha de Salida
5	Misional / Servicios	F705.22 base de datos clientes	Información	Servidor file server/documentos/5-clientes\base de datos clientes	Alejandra Barragán	Base datos de los clientes activos con que cuenta la empresa.	18/01/2014	N/A
6	Misional / Servicios	F702.04 k residual	Información	Servidor file server/documentos/5-clientes\5-clientes\clientes	Alejandra Barragán	Base datos donde se lleva un registro y control del estado económico de los contratos activos de la empresa.	8/06/2016	N/A
7	Misional / Servicios	Consolidado de brigadas de mantenimiento	Información	Servidor file server/documentos/5-clientes\5-clientes\clientes	Alejandra Barragán	Base de datos donde se registran los equipos y/o elementos intervenidos en una brigada de mantenimiento preventivo.	10/09/2016	N/A
8	Misional / Servicios	F705.19 base de servicio	Información	Servidor file server/documentos/5-clientes\5-clientes\clientes\carpeta cliente	Alejandra Barragán	Base de datos donde se registra los servicios realizados a la entidad.	N/A	N/A

Cuadro 5. (Continuación)

ID	Proceso	Nombre del Activo	Tipo	Ubicación	Propietario	Descripción	Gestión	
							Fecha de Ingreso	Fecha de Salida
9	Misional/ Servicios	F705.21 Seguimientos cotizaciones realizadas	Información	Servidor file server/documentos\administrativa\5-clientes\clientes\carpeta\3-consolidado de facturación\seguimiento bolsa de repuestos	Alejandra Barragán	Base de datos donde se registra las cotizaciones realizadas a cada cliente.	N/A	N/A
10	Misional/ Servicios	Consolidado de facturación clientes	Información	Servidor file server/documentos\administrativa\5-clientes\clientes\carpeta\3-consolidado de facturación\	Alejandra Barragán	Base de datos donde se consolida la facturación desde el inicio hasta el final de los contratos con entidades.	11/05/2015	N/A
11	Misional / Servicios	Anexos	Información	Servidor file server/documentos\administrativa\5-clientes\clientes\carpeta\3-consolidado de facturación\anexos	Alejandra Barragán	Se almacenan las facturas realizadas indicadas con su respectivo número de identificación.	18/01/2014	N/A
12	Misional / Servicios	Consolidado de facturación clientes	Información	Servidor file server/documentos\administrativa\5-clientes\clientes\carpeta\3-consolidado de facturación\	Alejandra Barragán	Base de datos donde se consolida la facturación de acuerdo al cliente.	14/08/2015	N/A

Cuadro 5. (Continuación)

ID	Proceso	Nombre del Activo	Tipo	Ubicación	Propietario	Descripción	Gestión	
							Fecha de Ingreso	Fecha de Salida
13	Misional / Servicios	Acta de inicio del contrato	Información	Servidor file server/documentos\administrativa\5-clientes\clientes\carpeta\5-documentos	Alejandra Barragán	Copia del acta de inicio de un contrato.	N/A	N/A
14	Misional/ Servicios	Contratos	Información	Servidor file server/documentos\administrativa\5-clientes\clientes\carpeta\5-documentos	Alejandra Barragán	Copia del contrato	N/A	N/A
15	Misional/ Servicios	F702.02 información general de un contrato	Información	Servidor file server/documentos\administrativa\5-clientes\clientes\carpeta\5-documentos	Alejandra Barragán	Formato que indica la información más relevante de un contrato a dar ejecución.	N/A	N/A
16	Misional/ Servicios	Oferta económica	Información	Servidor file server/documentos\administrativa\5-clientes\clientes\carpeta\5-documentos	Alejandra Barragán	Información económica y precisa de un contrato.	N/A	N/A

Cuadro 5. (Continuación)

ID	Proceso	Nombre del Activo	Tipo	Ubicación	Propietario	Descripción	Gestión	
							Fecha de Ingreso	Fecha de Salida
17	Misional/ Servicios	Oferta técnica	Información	Servidor file server/documentos\administrativa\5-clientes\clientes\carpeta\5-documentos	Alejandra Barragán	Información técnica y precisa de un contrato.	N/A	N/A
18	Misional/ Servicios	Pólizas	Información	Servidor file server/documentos\administrativa\5-clientes\clientes\carpeta\5-documentos	Alejandra Barragán	Pólizas generadas por los contratos en sus diferentes etapas (contrato inicial, adición y/u otro sí).	N/A	N/A
19	Misional/ Servicios	Escaneados radicados	Información	Servidor file server/documentos\administrativa\5-clientes\clientes\carpeta\5-documentos	Alejandra Barragán	Se almacenan los documentos firmados y digitalizados generados durante la ejecución del contrato.	N/A	N/A
20	Misional/ Servicios	Estudio de mercado	Información	Servidor file server/documentos\administrativa\5-clientes\clientes\carpeta\6-consecutivos estudios de mercado\estudio de mercado	Alejandra Barragán	Se almacenan los estudios de mercados realizados durante el año.	N/A	N/A

Cuadro 5. (Continuación)

ID	Proceso	Nombre del Activo	Tipo	Ubicación	Propietario	Descripción	Gestión	
							Fecha de Ingreso	Fecha de Salida
21	Misional/ Servicios	Cotizaciones aprobadas	Información	Servidor file server/documentos\administrativa\5-clientes\clientes\carpeta\7-cotizaciones	Alejandra Barragán	Se almacenan las cotizaciones que se han aprobado en el año.	N/A	N/A
22	Misional/ Servicios	Cotizaciones generales	Información	Servidor file server/documentos\administrativa\5-clientes\clientes\carpeta\7-cotizaciones	Alejandra Barragán	Se almacenan las cotizaciones realizadas en el año.	N/A	N/A
23	Misional/ Servicios	Cotizaciones pdf	Información	Servidor file server/documentos\administrativa\5-clientes\clientes\carpeta\7-cotizaciones	Alejandra Barragán	Se almacenan las cotizaciones enviadas a los clientes.	N/A	N/A
24	Misional/ Servicios	F705.02 cronograma de brigadas de mantenimiento preventivo	Información	Servidor file server/documentos\administrativa\5-clientes\clientes\carpeta\8-cronograma general de clientes	Alejandra Barragán	Base general donde se registra la programación de las brigadas de mantenimiento preventivo de los activos de todos los clientes activos de la	24/01/2014	N/A

						empresa.		

Cuadro 5. (Continuación)

ID	Proceso	Nombre del Activo	Tipo	Ubicación	Propietario	Descripción	Gestión	
							Fecha de Ingreso	Fecha de Salida
25	Misional/ Servicios	Autorización de pago	Información	Servidor file server/documentos\administrativa\5-clientes\clientes\carpeta\9-pagos	Alejandra Barragán	Se almacenan las cartas generadas para autorizar el pago de los técnicos que colaboraron en la ejecución de una brigada.	N/A	N/A
26	Apoyo/ Tesorería	Facturación y comprobantes contables	Información	Servidor file server/documentos\tesorería\facturas	Andrés Ramírez	Se almacena la información de facturación y comprobantes contables.	N/A	N/A
27	Apoyo/ Tesorería	Consignaciones de dinero recaudado	Información	Servidor file server/documentos\tesorería\consignaciones	Andrés Ramírez	Se almacena la información de consignaciones de dinero recaudado.	N/A	N/A
28	Apoyo/ Tesorería	Recaudo de cartera	Información	Servidor file server/documentos\tesorería\recaudo cartera	Andrés Ramírez	Se almacena la información de recaudo de	N/A	N/A

						cartera. Se establece 60 días calendario a clientes oficiales y 45 días calendario a clientes particulares.		

Cuadro 5. (Continuación)

ID	Proceso	Nombre del Activo	Tipo	Ubicación	Propietario	Descripción	Gestión	
							Fecha de Ingreso	Fecha de Salida
29	Apoyo/ Compras	Listado de proveedores	Información	Servidor file server/documentos\compras\proveedores	May González	Se almacena información del listado de proveedores calificados, selección y evaluación de proveedores.	N/A	N/A
30	Apoyo/ Compras	Listado de recursos físicos	Información	Servidor file server/documentos\almacén\recursos	May González	Se almacena información de los recursos que, recibidos, verificación y entrega de suministros comprados.	N/A	N/A

31	Apoyo/ Gestión humana	Requisición de personal	Información	Servidor file server/documentos\ghumana\contratación	Leonardo Abril	Se almacena la información de reclutamiento, selección y contratación de personal.	N/A	N/A
32	Apoyo/ Gestión humana	Evaluación de desempeño	Información	Servidor file server/documentos\ghumana\evaluaciondesempeño	Leonardo Abril	Se almacena la información de la evaluación de desempeño a todo el personal de la empresa.	N/A	N/A

Cuadro 5. (Continuación)

ID	Proceso	Nombre del Activo	Tipo	Ubicación	Propietario	Descripción	Gestión	
							Fecha de Ingreso	Fecha de Salida
33	Estratégicos/ Calidad	Informe de auditoría interna	Información	Servidor file server/documentos\gcalidad\auditoriainterna	Leonardo Abril	Se almacenan los informes de auditoría interna y el análisis de las deficiencias en las etapas de prestación de servicio.	N/A	N/A
34	Estratégicos/ Calidad	Indicadores de gestión	Información	Servidor file server/documentos\gcalidad\indicadoresgestion	Leonardo Abril	Se almacena el informe del análisis de indicadores de gestión para tomar acciones preventivas y correctivas.	N/A	N/A

35	Estratégicos/ Gerencial	Plan estratégico	Información	Servidor file server/documentos\gcalidad\indicadoresgestion	Andrea Castillo	Se almacena el desarrollo del plan estratégico de la empresa, el seguimiento y los resultados de los indicadores de gestión.	N/A	N/A
36	Apoyo/ Sistemas	Firewall herramienta Smoothwall	Software	Se encuentra instalado en un servidor ubicado en el Datacenter	Jefferson Rodríguez	Firewall de seguridad en la red.	7/05/2011	9/11/2016

Cuadro 5. (Continuación)

ID	Proceso	Nombre del Activo	Tipo	Ubicación	Propietario	Descripción	Gestión	
							Fecha de Ingreso	Fecha de Salida
37	Apoyo/ Sistemas	Soporte Aranda Service Desk T&SCOMP	Software	Se encuentra instalado en un servidor ubicado en el Datacenter	Jefferson Rodríguez	Herramienta para el control de mesa de servicio.	4/02/2011	N/A
38	Apoyo/ Sistemas	MI.COM.CO servicio de Hosting Linux tyscomp.com	Servicio	En la nube	Jefferson Rodríguez	Hosting donde se encuentra la página alojada (www.tyscomp.com).	12/07/2013	12/07/2016
39	Apoyo/ Sistemas	MI.COM.CO servicio de Dominio tyscomp.com	Servicio	En la nube	Jefferson Rodríguez	Administración de Dominio.	18/01/2008	N/A

40	Apoyo/ Sistemas	Suscripción y Hosting WIX	Servicio	En la nube	Jefferson Rodríguez	Hosting donde se encuentra alojada actualmente la página de T&S COMP. Tecnología y Servicios.	20/06/2016	N/A
41	Apoyo/ Sistemas	Microsoft Partner	Servicio	En la nube	Jefferson Rodríguez	Suscrición Partner Microsoft (solo se actualizan datos).	30/04/3016	N/A
42	Apoyo/ Sistemas	Microsoft Partner Action Pack (Licencias)	Software	En la nube	Jefferson Rodríguez	Suscripción por un (1) año a action pack (licencias y software de uso interno) promedio 395 USD.	21/02/2012	N/A

Cuadro 5. (Continuación)

ID	Proceso	Nombre del Activo	Tipo	Ubicación	Propietario	Descripción	Gestión	
							Fecha de Ingreso	Fecha de Salida
43	Apoyo/ Sistemas	Antivirus AVG Internet Security 2013	Software	En la nube	Jefferson Rodríguez	Licencia para 25 computadores incluyendo servidores.	22/04/2013	22/04/2016
44	Apoyo/ Tesorería	Helisa	Software	Se encuentra instalado en un servidor ubicado en el datacenter	Andrés Ramírez	Software contable. Sin Soporte, pago adicional por este.	8/07/2011	N/A

45	Apoyo/ Tesorería	Aplicativo Helisa nomina	Software	Se encuentra instalado en un servidor ubicado en el datacenter	Andrés Ramírez	Aplicativo HELISA NOMINA de 1-100 empleados con 3 sesiones	28/06/2016	N/A
46	Apoyo/ Sistemas	Aranda Service Desk T&SCOMP	Software	Se encuentra instalado en un servidor ubicado en el datacenter	Jefferson Rodríguez	Aranda service desk x 2 concurrentes con soporte e ingeniero de soluciones	4/02/2011	N/A
47	Apoyo/ Sistemas	Cloudberry	Software	Se encuentra instalado en el servidor de archivos	Jefferson Rodríguez	Licencia perpetua complemento conector amazon gestor de backup	11/12/2014	N/A
48	Apoyo/ Sistemas	Network Inventory	Software	En la nube	Jefferson Rodríguez	Licencia para 300 nodos	31/12/2014	N/A

Cuadro 5. (Continuación)

ID	Proceso	Nombre del Activo	Tipo	Ubicación	Propietario	Descripción	Gestión	
							Fecha de Ingreso	Fecha de Salida

49	Misional/ Comercial Misional/ Servicios Estratégicos/ Gerencial Estratégicos/ Calidad Apoyo/ Tesorería Apoyo/ Compras Apoyo/ Gestión humana Apoyo/ Sistemas	Computadores de escritorio	Hardware	Oficinas T&S COMP. Tecnología y Servicios.	Todos los procesos	16 computadores de escritorio	N/A	N/A
50	Estratégicos/ Gerencial	Portátil	Hardware	Oficina de la gerencia T&S COMP. Tecnología y Servicios.	Andrea Castillo	2 portátiles	N/A	N/A
51	Apoyo/ Sistemas	Servidores	Hardware	Ubicado en el Datacenter de T&S COMP. Tecnología y Servicios.	Jefferson Rodríguez	2 Servidores 4 Equipos que actúan como servidores	N/A	N/A
52	Apoyo/ Sistemas	Impresoras	Hardware	Oficina T&S COMP. Tecnología y Servicios.	Jefferson Rodríguez	4 impresoras ubicadas en cada uno de los pisos de la empresa.	N/A	N/A

Cuadra 5. (Continuación)

ID	Proceso	Nombre del Activo	Tipo	Ubicación	Propietario	Descripción	Gestión	
							Fecha de Ingreso	Fecha de Salida

53	Apoyo/ Sistemas	Escáner	Hardware	Oficina T&S COMP. Tecnología y Servicios.	Jefferson Rodríguez	2 escáner ubicados los pisos 1 y 2 de la empresa.	N/A	N/A
54	Apoyo/ Sistemas	DVR (CCTV)	Hardware	Oficina T&S COMP. Tecnología y Servicios.	Jefferson Rodríguez	Circuito cerrado de televisión ubicado en las instalaciones de la compañía.	N/A	N/A
55	Misional/ Comercial Misional/ Servicios Estratégicos/ Gerencial Estratégicos/ Calidad Apoyo/ Tesorería Apoyo/ Compras Apoyo/ Gestión humana Apoyo/ Sistemas	Funcionarios	Recurso Humano	Oficina T&S COMP. Tecnología y Servicios.	N/A	La empresa cuenta con 22 funcionarios que hacen parte de las áreas de gestión gerencial y de calidad, Servicios y comercial, Facturación, recaudo, compras y almacén, Gestión humana y Sistemas.	N/A	N/A
56	Apoyo/ Sistemas	Datacenter	Instalaciones	Oficina T&S COMP. Tecnología y Servicios.	Jefferson Rodríguez	Ingresa únicamente el administrador de los sistemas de información.	N/A	N/A

Cuadro 5. (Continuación)

ID	Proceso	Nombre del	Tipo	Ubicación	Propietario	Descripción	Gestión

		Activo					Fecha de Ingreso	Fecha de Salida
57	Apoyo/ Sistemas	Router	Hardware	Oficina T&S COMP. Tecnología y Servicios.	Jefferson Rodríguez	Se cuentan con 2 equipos usados para interconectar sistemas de información.	N/A	N/A
58	Apoyo/ Sistemas	Switch	Hardware	Oficina T&S COMP. Tecnología y Servicios.	Jefferson Rodríguez	Se cuentan con 2 equipos de telecomunicaciones usados para interconectar sistemas de información.	N/A	N/A
59	Misional/ Comercial	Proveedores	Recurso humano	Oficina T&S COMP. Tecnología y Servicios.	N/A	La empresa cuenta con un promedio de 90 proveedores, quienes hacen parte del proceso comercial.	N/A	N/A
60	Misional/ Comercial	Clientes	Recurso humano	Oficina T&S COMP. Tecnología y Servicios.	N/A	La empresa cuenta con un promedio de 300 a 400 clientes, quienes hacen parte del proceso comercial.	N/A	N/A
Fuente: Autores. Información brindada por T&S COMP.								

6.2 VALORACIÓN DE ACTIVOS EN T&S COMP. TECNOLOGÍA Y SERVICIOS S.A.S

Para alcanzar el objetivo de valorar los activos críticos de la empresa, se debe tener en cuenta que cuanta mayor criticidad tenga el recurso, mayor será el riesgo al que está expuesto, por esta razón, en el momento que se presente un evento, la amenaza se puede materializar y puede causar grandes impactos para la organización.

En un modelo de negocio orientado a la prestación de servicios tecnológicos, para efectos del diseño del SGSI en T&S COMP. Tecnología y Servicios S.A.S, la valoración de los activos de información se determinará de acuerdo a los principios de seguridad de la información y a los niveles de protección adecuados basados en su valor, como se observa en los cuadros 6, 7 y 8, en donde están las escalas de valoración de los principios de seguridad de la información:

- **Confidencialidad**: Se definen en los siguientes niveles:

Cuadro 6. Clasificación según la confidencialidad.

Tipo	Significado
Información Pública Reservada	Datos o información que sólo se encuentra disponible para sólo un proceso de la empresa. En caso que un tercero acceda sin autorización a esta información puede causar impacto negativo: financiero, legal, operativo o reputacional.
Información Pública Clasificada	Datos o información que se encuentra disponible para todos los procesos de la empresa. En caso que un tercero acceda sin autorización a esta información puede causar un impacto negativo a todos los procesos.
Información Pública	Datos o información que se encuentra disponible para todos los procesos de la empresa y puede ser publicada o entregada a cualquier persona externa. No genera daños a terceros ni a las actividades llevadas a cabo por la empresa.
No Clasificada	Activos que no se encuentran incluidos en el inventario y que no han sido clasificados.
Fuente: MINTIC[35]	

[35] MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Guía para la Gestión y Clasificación de Activos de Información. Clasificación de activos de la información.

- **Integridad**: Se definen en los siguientes niveles:

Cuadro 7. Clasificación según la integridad.

Estado	Significado
Alta	Pérdida de completitud de datos o información, puede causar impacto negativo: financiero, legal, operativo o reputacional de forma crítica.
Medio	Pérdida de completitud de datos o información, puede causar impacto negativo: financiero, legal, operativo o reputacional de forma moderada.
Bajo	Pérdida de completitud de datos o información, puede causar impacto negativo: financiero, legal, operativo o reputacional de forma baja.
No Clasificada	Activos que no se encuentran incluidos en el inventario y que no han sido clasificados.
Fuente: MINTIC[36]	

- **Disponibilidad**: Se definen en los siguientes niveles:

Cuadro 8. Clasificación según la disponibilidad.

Estado	Significado
Alta	Indisponibilidad total datos o información puede causar impacto negativo: financiero, legal, operativo o reputacional de forma crítica.
Medio	Indisponibilidad datos o información puede causar impacto negativo: financiero, legal, operativo o reputacional de forma moderada.
Bajo	Indisponibilidad datos o información puede afectar la operación, pero no causa un impacto negativo: financiero, legal, operativo o reputacional.
No Clasificada	Activos que no se encuentran incluidos en el inventario y que no han sido clasificados.
Fuente: MINTIC[37]	

[36] Ibíd.,
[37] Ibíd.,

En el cuadro 9 se determina la criticidad de los activos de T&S COMP. Tecnología y Servicios S.A.S de acuerdo a la escala de valoración de los principios de seguridad indicados anteriormente.

Para el cuadro se registran los siguientes campos:

- **Identificador:** Número de identificación del activo.

- **Nombre del Activo:** Nombre del activo de información de acuerdo al proceso al que pertenece.

- **Principio**: Protección de la información de acuerdo a la Confidencialidad, Integridad y Disponibilidad del activo de información.

- **Clasificación:** Valoración de los activos de acuerdo a la criticidad de pérdida del principio de seguridad de la información.

- **Justificación**: Impacto que causaría la pérdida de Confidencialidad, Integridad o Disponibilidad del activo.

Cuadro 9. Valoración de Activos T&S COMP. Tecnología y Servicios S.A.S.

ID	Nombre del activo	Tipo	Principio	Clasificación	Justificación
1	Informe mensual gerencia.	Información	Integridad	Media	La pérdida de integridad de este activo afectaría la operación y la reputación del proceso de servicios, ya que es el consolidado mensual de lo trabajado con sus resultados finales.
2	Indicadores administrativa y servicio	Información	Integridad	Media	La pérdida de integridad de este activo no causa un impacto financiero ni operacional, sin embargo, es importante su disponibilidad ya que es la base para medir los indicadores.
3	Localización archivo físico administrativa y servicios	Información	Disponibilidad	Alta	La pérdida de este activo, puede afectar tanto financiera como operacionalmente ya que aquí se registra la ubicación final del archivo físico de este proceso.
4	Ubicación general archivo físico general de la empresa	Información	Disponibilidad	Media	La pérdida de este activo, puede afectar tanto financiera como operacionalmente ya que aquí se registra la ubicación final del archivo físico de la empresa.
5	F705.22 base de datos clientes	Información	Confidencialidad	Información Pública Reservada	La pérdida de este activo, afectaría gravemente la parte financiera y operacional de la empresa ya que en este se tiene registrado los datos de todos los clientes que se encuentran activos en la empresa.
6	F702.04 k residual	Información	Confidencialidad	Información Pública Reservada	La pérdida de este activo, afectaría gravemente la parte financiera y operacional de la empresa ya que en este se lleva un consolidado de la parte económica de los contratos actuales de la empresa.
7	Consolidado de brigadas de mantenimiento	Información	Integridad	Alta	La pérdida de este documento afectaría la parte operacional de un contrato, ya que en este se consolida las brigadas preventivas que se deben cumplir contractualmente.

Cuadro 9. (Continuación)

ID	Nombre del activo	Tipo	Principio	Clasificación	Justificación
8	F705.19 base de servicio	Información	Integridad	Alta	La pérdida de este documento afectaría la parte operacional de un contrato, ya que en este se consolida los servicios prestados al mismo.
9	F705.21 Seguimientos cotizaciones realizadas	Información	Confidencialidad	Información Pública Reservada	La pérdida de este documento afectaría gravemente la parte financiera y operacional, ya que en esta se registra las partes y servicios cotizados y aprobados en un contrato para futuras facturaciones.
10	Consolidado de facturación clientes	Información	Confidencialidad	Información Pública Reservada	La pérdida de este documento tendría un impacto alto ya que en él se consolida la facturación generada en un contrato desde el inicio de su ejecución hasta el fin.
11	Anexos	Información	Confidencialidad	Información Pública Reservada	La pérdida de este documento tendría una afectación media, ya que en el sistema contable se pueden reimprimir las facturas.
12	Consolidado de facturación clientes	Información	Confidencialidad	Información Pública Reservada	La pérdida de este documento afectaría la operación de un contrato ya que no se tendría oportunamente el consolidado de facturación del mismo.
13	Acta de inicio del contrato	Información	Confidencialidad	Información Pública Reservada	La pérdida de este documento tendría un impacto moderado en la operación, ya que se tiene una copia en físico.

Cuadro 9. (Continuación)

ID	Nombre del activo	Tipo	Principio	Clasificación	Justificación
14	Contratos	Información	Confidencialidad	Información Pública Reservada	La pérdida de este documento tendría un impacto moderado en la operación ya que se tiene una copia en físico.
15	F702.02 información general de un contrato	Información	Disponibilidad	Baja	La pérdida de este documento seria de un impacto bajo, ya que esto solo es a manera de informativo.
16	Oferta económica	Información	Disponibilidad	Baja	La pérdida de este documento seria de un impacto bajo, ya que esto solo es a manera de informativo.
17	Oferta técnica	Información	Disponibilidad	Baja	La pérdida de este documento seria de un impacto bajo, ya que esto solo es a manera de informativo.
18	Pólizas	Información	Confidencialidad	Información Pública Reservada	La pérdida de estos documentos tendría un impacto alto ya que son el soporte tanto para la presentación de una licitación como el soporte para hacer efectiva de la misma cuando sea necesario.
19	Escaneados radicados	Información	Integridad	Alta	La pérdida de estos documentos, tendría un impacto mayor ya que son los soportes de los documentos que se entregaron con su respectiva firma de recibido.
20	Estudio de mercado	Información	Confidencialidad	Información Pública Reservada	La pérdida de estos documentos, tendría un impacto mayor ya que son los soportes de los documentos que se entregaron con su respectiva firma de recibido.
21	Cotizaciones aprobadas	Información	Confidencialidad	Información Pública Reservada	La pérdida de estos documentos, tendría un impacto mayor ya que son los soportes de los documentos que se entregaron con su respectiva firma de recibido.

Cuadro 9. (Continuación)

ID	Nombre del activo	Tipo	Principio	Clasificación	Justificación
22	Cotizaciones generales	Información	Confidencialidad	Información Pública Reservada	La pérdida de estos documentos tendría un impacto mayor ya que son los soportes de los documentos que se entregaron con su respectiva firma de recibido.
23	Cotizaciones pdf	Información	Confidencialidad	Información Pública Reservada	La pérdida de estos documentos tendría un impacto mayor ya que son los soportes de los documentos que se entregaron con su respectiva firma de recibido.
24	F705.02 cronograma de brigadas de mantenimiento preventivo	Información	Integridad	Alta	La pérdida de integridad de este documento tendría un impacto alto ya que contiene información de las fechas de brigada de mantenimiento de los activos de los clientes.
25	Autorización de pago	Información	Confidencialidad	Información Pública Reservada	La pérdida de confidencialidad de estos documentos tendría un impacto alto ya que son las cartas generadas para autorizar el pago de los técnicos que colaboraron en la ejecución de una brigada.
26	Facturación y comprobantes contables	Información	Confidencialidad	Información Pública Reservada	La pérdida de confidencialidad de estos documentos tendría un impacto alto ya que es la información de facturación y comprobantes contables.
27	Consignaciones de dinero recaudado	Información	Confidencialidad	Información Pública Reservada	La pérdida de confidencialidad de estos documentos tendría un impacto alto ya que es la información de las consignaciones de dinero recaudado.
28	Recaudo de cartera	Información	Confidencialidad	Información Pública Reservada	La pérdida de confidencialidad de estos documentos tendría un impacto alto ya que es la información del recaudo de cartera.

Cuadro 9. (Continuación)

ID	Nombre del activo	Tipo	Principio	Clasificación	Justificación
29	Listado de proveedores	Información	Integridad	Alta	La pérdida de integridad de estos documentos tendría un impacto alto ya que es la información del listado de proveedores calificados, selección y evaluación de proveedores.
30	Listado de recursos físicos	Información	Disponibilidad	Media	La pérdida de disponibilidad de estos documentos tendría un impacto medio ya que es la información de los recursos recibidos, verificación y entrega de suministros comprados.
31	Requisición de personal	Información	Integridad	Alta	La pérdida de integridad de estos documentos tendría un impacto alto ya que se encuentran las hojas de vida de los empleados, la información reclutamiento, selección y contratación de personal.
32	Evaluación de desempeño	Información	Disponibilidad	Media	La pérdida de disponibilidad de estos documentos tendría un impacto medio ya que se encuentra la información de evaluación de desempeño de todo el personal de la empresa.
33	Informe de auditoría interna	Información	Confidencialidad	Información Pública Reservada	La pérdida de confidencialidad de estos documentos tendría un impacto alto ya que los informes de auditoría interna y el análisis de las deficiencias en las etapas de prestación de servicio siempre deben estar disponible sólo para el proceso estratégico de la empresa.
34	Indicadores de gestión	Información	Confidencialidad	Información Pública Reservada	La pérdida de confidencialidad de estos documentos tendría un impacto alto ya que los indicadores de gestión siempre deben estar disponible sólo para el proceso estratégico de la empresa.

35	Plan estratégico	Información	Confidencialidad	Información Pública Clasificada	La pérdida de confidencialidad de estos documentos tendría un impacto medio ya que el plan estratégico debe ser conocido por todos los procesos de la empresa.

Cuadro 9. (Continuación)

ID	Nombre del activo	Tipo	Principio	Clasificación	Justificación
36	Firewall herramienta Smoothwall	Software	Disponibilidad	Alta	La pérdida de este software genera gran impacto ya que se desprotegería la red de la compañía
37	Soporte Aranda Service Desk T&SCOMP	Software	Disponibilidad	Alta	La pérdida de este software genera impacto alto ya que no se tendría acceso para el control de servicio de mesa de ayuda.
38	MI.COM.CO servicio de Hosting Linux tyscomp.com	Servicio	Disponibilidad	Alta	La pérdida de estos documentos, tendría un impacto mayor ya que es la página web principal de la compañía.
39	MI.COM.CO servicio de Dominio tyscomp.com	Servicio	Disponibilidad	Alta	La pérdida de estos documentos, tendría un impacto mayor ya que es la página web principal de la compañía.
40	Suscripción y Hosting WIX	Servicio	Disponibilidad	Alta	La pérdida de este servicio generaría impacto alto ya que es el hosting donde se encuentra alojada actualmente la página de T&S COMP. Tecnología y Servicios.
41	Microsoft Partner	Servicio	Disponibilidad	Alta	La pérdida de este servicio generaría impacto alto, teniendo en cuenta que este servicio está en la nube, no se podría tener o ver la información.
42	Microsoft Partner Action Pack (Licencias)	Software	Disponibilidad	Alta	La pérdida de este servicio generaría impacto alto, teniendo en cuenta que este servicio está en la nube, no se podría tener o ver la información.
43	Antivirus AVG Internet Security 2013	Software	Disponibilidad	Alta	La pérdida de disponibilidad de este software generaría impacto alto ya que los recursos quedarían desprotegidos y podrían ser afectados por ataques informáticos.

44	Helisa	Software	Confidencialidad	Información Pública Reservada	La pérdida de este recurso tendría un impacto mayor ya que este software contable solo debe estar disponible para el contador de la empresa.

Cuadro 9. (Continuación)

ID	Nombre del activo	Tipo	Principio	Clasificación	Justificación
45	Aplicativo Helisa nomina	Software	Confidencialidad	Información Pública Reservada	La pérdida de este recurso tendría un impacto mayor ya que este software contable solo debe estar disponible para el contador de la empresa.
46	Aranda Service Desk T&SCOMP	Software	Disponibilidad	Alta	La pérdida de este software genera impacto alto ya que no se tendría acceso para el control de servicio de soporte para los clientes de la organización.
47	Cloudberry	Software	Disponibilidad	Alta	La pérdida de este recurso tendría un impacto alto ya que es el gestor de backup de los archivos generados a partir de las actividades realizadas por los funcionarios de la organización.
48	Network Inventory	Software	Confidencialidad	Información Pública Reservada	La pérdida de este recurso tendría un impacto mayor ya que este software permite realizar el seguimiento de las versiones de software y licencias de los ordenadores y solo debe estar disponible para el ingeniero de TI de la empresa.
49	Computadores de escritorio	Hardware	Disponibilidad	Alta	La indisponibilidad de este recurso generaría un impacto alto ya que se detendría la operación de las actividades de la empresa.
50	Portátil	Hardware	Disponibilidad	Baja	La indisponibilidad de este recurso generaría un impacto bajo ya que no almacena información sensible.

51	Servidores	Hardware	Disponibilidad	Alta	La indisponibilidad de este recurso generaría un impacto alto ya que en los servidores se almacena toda la información de las actividades de la empresa.

Cuadro 9. (Continuación)

ID	Nombre del activo	Tipo	Principio	Clasificación	Justificación
52	Impresoras	Hardware	Disponibilidad	Media	La indisponibilidad de este recurso generaría un impacto medio ya que la mayoría de información es almacenada por medio digital.
53	Escáner	Hardware	Disponibilidad	Alta	La indisponibilidad de este recurso generaría un impacto alto ya que se escanean todos los documentos físicos para ser almacenados digitalmente.
54	DVR (CCTV)	Hardware	Disponibilidad	Alta	La indisponibilidad de este hardware generaría un impacto alto ya que por medio de este recurso se ejerce control y monitoreo para la seguridad de los activos de la empresa.
55	Funcionarios	Recurso Humano	Disponibilidad	Alta	La falta de funcionarios en la compañía genera impacto alto ya que son la parte fundamental para que las actividades se lleven eficazmente.
56	Datacenter	Instalaciones	Disponibilidad	Alta	La pérdida de disponibilidad de este recurso genera impacto alto ya que se detendrían las actividades realizadas por los funcionarios de la organización.
57	Router	Red	Disponibilidad	Alta	La pérdida de disponibilidad de este recurso, genera un impacto alto, teniendo en cuenta que no habría conexión, ni transmisión de datos, ni recepción de los mismos.

58	Switch	Red	Disponibilidad	Alta	La pérdida de disponibilidad de este recurso, genera un impacto alto, ya que no existirá conexión entre los diferentes equipos, conectados a la misma red.

Cuadro 9. (Continuación)

ID	Nombre del activo	Tipo	Principio	Clasificación	Justificación
59	Proveedores	Recurso Humano	Disponibilidad	Alta	La falta de proveedores, en la empresa generaría un impacto alto diferentes procesos, en donde son necesarios sus servicios.
60	Clientes	Recurso humano	Confidencialidad	Información Pública Reservada	La falta de clientes y la pérdida de la información suministrada, genera pérdida de confianza, y vulnera la imagen de la empresa. Adicionalmente, genera un impacto financiero a la compañía
Fuente: Autores. Información suministrada por T&S COMP.					

7. GESTIÓN Y ANÁLISIS DE RIESGOS DE LA SEGURIDAD

Como parte del SGSI en T&S COMP. Tecnología y Servicios S.A.S., se deben considerar los riesgos a los que está expuesta la empresa y determinar oportunidades para lograr los resultados deseados, prevenir eventos indeseados y obtener una mejora continua mediante la evaluación e implementación de acciones previstas en el tratamiento de los riesgos, con el objetivo de asegurar la integridad, disponibilidad y confidencialidad de la información en un modelo de negocio orientado a la prestación de servicios tecnológicos.

Para la administración adecuada de los riesgos en los procesos de Apoyo, Misionales y Estratégicos de T&S COMP. Tecnología y Servicios S.A.S, como primera medida, se obtuvo el compromiso de la alta dirección, el cual brindó el respaldo para la identificación, evaluación y tratamiento de riesgos, determinó controles y asignó recursos necesarios para su gestión. Por otro lado, se conformó un grupo interdisciplinario encargado de liderar el proceso del SGSI y el posterior análisis de los riesgos, con gran conocimiento en los procesos de la entidad y el canal directo de comunicación con la alta dirección y las otras dependencias.

En esta etapa, para efectos de análisis de riesgo en los procesos de Apoyo, Misionales y Estratégicos de T&S COMP. Tecnología y Servicios S.A.S, se utilizarán las metodologías ISO 31000 e ISO 27005, las cuales proveen las directrices para desarrollar adecuadamente la gestión de riesgos. Se establecerá conforme a los objetivos de la empresa y de acuerdo sus necesidades para el mejoramiento del gobierno de Seguridad de la Información.

7.1 ANÁLISIS DE RIESGOS

7.1.1 Identificación de Riesgo. En esta etapa, la identificación del riesgo se realiza con base en los elementos establecidos en el Contexto y el estado actual de la empresa T&S COMP. Tecnología y Servicios S.A.S, la identificación y valoración de activos analizados previamente en el capítulo anterior, para determinar los factores que pueden interrumpir el cumplimiento de los objetivos del negocio. Éstas pueden ser internas o externas.

Se deben definir fuentes de riesgo, eventos y causas para realizar una lista de riesgos con el objetivo de prevenir, mejorar y crear controles para evitar que puedan afectar el desarrollo óptimo de las actividades de empresa. Adicionalmente, se deben considerar posibles escenarios que demuestren lo que podría suceder en un momento de adversidad y que puede comprometer la Seguridad de la Información.

7.1.2 Identificación de amenazas. Las amenazas son acciones que aprovechan una vulnerabilidad y pueden causar daños potenciales a los activos de información de la empresa. Existen diferentes fuentes de amenazas que se listan en el cuadro 10, tomando como referencia la norma ISO 27005 Anexo C:

Cuadro 10. Fuente de las amenazas

Fuente	Identificación	Descripción
Accidental	A	Daño accidental a los activos de información.
Deliberado	D	Daño voluntario o intencionado a los activos de información.
Ambiental	E	Daño de origen natural y no por acciones humanas.
Fuente: Autores. Tomado como referencia la norma ISO 27005 Anexo C.		

Una vez identificadas las fuentes de amenazas, en el cuadro 11 se indican las amenazas más comunes en la empresa:

Cuadro 11. Identificación de amenazas T&S COMP. Tecnología y Servicios S.A.S.

Tipo	Amenaza	Fuente
Fenómenos naturales	Terremotos Inundaciones Climatológicos Volcánicos	E
Daño Físico	Fuego Destrucción de dispositivos Polvo Corrosión Agua Contaminación	D A E
Fallas en dispositivos informáticos	Fallas de dispositivo Fallas en el funcionamiento del hardware Fallas en el funcionamiento del software	A
	Mal manejo del dispositivo	A

Cuadro 11. (Continuación)

Tipo	Amenaza	Fuente
Fallas en dispositivos informáticos	Inexistencia de mantenimientos de los sistemas de información	D
Pérdida de los servicios esenciales	Fallas en el suministro de servicios eléctricos	A D E
	Fallas en el suministro del servicio de agua Falla en suministros de telecomunicaciones	A D
Compromiso de la información	Robo de dispositivos Robo de documentos Espionaje remoto	A
	Divulgación de información confidencial Manipulación con software o hardware Datos procedentes de fuentes no fiables	A D
Actividades no autorizadas	Uso no autorizado del dispositivo Copia ilegal de información Copia ilegal de software	A
	Uso de software no licenciado	A D
Compromiso de las funciones	Abuso de derechos	A D
	Error en el uso de las funciones Negar acciones Falsificación de derechos Incumplimiento en la disponibilidad del personal	A
Fuente: Autores. Tomado como referencia la norma ISO 27005 Anexo C		

7.1.3 Identificación de vulnerabilidades. Las vulnerabilidades son debilidades de los activos de información que pueden ser aprovechados por un ciberdelincuente. Luego de determinar las amenazas más comunes, en la cuadro 12 se muestran las vulnerabilidades identificadas asociadas a la empresa, tomando como referencia la norma ISO 27005 Anexo D:

Cuadro 12. Vulnerabilidades T&S COMP. Tecnología y Servicios S.A.S

No.	Tipo de activo	Vulnerabilidad
1	Hardware	Susceptibilidad a la humedad, polvo y suciedad.
2		Ausencia de un eficiente control de cambios en la configuración.
3		Susceptibilidad a las variaciones de voltaje.
4		Susceptibilidad a las variaciones de temperatura.
5		Almacenamiento sin seguridad.
6		Utilización inapropiada de dispositivos.
7	Software	Desactualización de software.
8		Ausencia de bloqueo de equipo cuando se abandona la estación de trabajo.
9		Gestión deficiente de las contraseñas.
10		Descarga y uso no controlado de software.
11	Red	Falla del canal principal.
12		Arquitectura de red insegura.
13	Personal	Ausencia del personal.
14		Desconocimiento en seguridad de la información.
15		Uso incorrecto de software y hardware.
16		Falta de conciencia en materia de seguridad de la información.
17		Ausencia de procedimiento formal para el registro de ingreso y retiro de personas externas.
18		Desactualización de inventario de activos de información.
19		Pérdida de confidencialidad en las propuestas licitatorias entregados por un empleado a un tercero (competencia).
20		Pérdida o daño de activos de propiedad del contratante por inadecuadas prácticas al momento de realizar mantenimiento por parte del funcionario que ejecuta la actividad.

Cuadro 12. (Continuación)

No.	Tipo de activo	Vulnerabilidad
21	Personal	Consulta en páginas web sobre términos de referencia en procesos licitatorios que puedan contener información falsa.
22		Pérdida de información contractual de los clientes accidental o provocado por parte de un empleado.
23	Información	Manejo indebido de información confidencial a la cual tienen acceso los empleados.
24		Divulgación no autorizada sobre la información de los clientes, generando pérdida de confianza en la compañía y acciones legales contra la misma.
25		Eliminación accidental o intencional de archivos que puede producir afectación en el desarrollo operacional de la compañía.
26		Modificación en información confidencial que se realiza de manera no autorizada, intencional o accidentalmente.
27		Pérdida de confidencialidad sobre información contractual de los clientes.
28	Organización	Conservar contraseñas de inicio de sesión en plataformas en las que se almacena información sensible.
29		Uso o divulgación de contraseñas inseguras como método de ataque para adquirir información confidencial.
30		Ausencia de controles para el manejo de la información personal.
31		Ausencia de controles en caso de incidentes de seguridad de la información.
32		Ausencia de políticas sobre limpieza de escritorio.
33		Ausencia del gobierno de seguridad de la información.
34		Ausencia de planes para la gestión de continuidad de negocio.

Fuente: Autores. Tomado como referencia la norma ISO 27005 Anexo D.

7.2 EVALUACIÓN DEL RIESGO

Al gestionar el riesgo, se debe valorar y determinar elementos para intervenir incidentes que puedan afectar la organización. El proceso de valoración de riesgos ayuda a estimar la magnitud de las amenazas que están presentes en la empresa y que a través de los planes de tratamiento se pueden tomar medidas preventivas o correctivas ante eventos que puedan causar daño.

Para evaluar los riesgos a los que está expuesta la empresa T&S COMP. Tecnología y Servicios S.A.S, se utilizará el análisis cuantitativo. Por lo tanto, se describe a continuación, en los cuadros 13 y 14, la probabilidad de ocurrencia y el impacto del riesgo.

Cuadro 13. Probabilidad de ocurrencia.

Valor	Criterio	Frecuencia	Descripción
1	Raro	Nunca ha ocurrido.	El evento puede suceder en situaciones extrañas.
2	Improbable	Una vez en el último año.	El evento puede suceder en cierto momento.
3	Posible	Una vez por semestre.	El evento posiblemente podría suceder en cierto momento.
4	Probable	Una vez por mes.	El evento probablemente sucederá en la mayoría de las situaciones.
5	Frecuente	Varias veces en el día.	El evento ocurrirá en la mayoría de las situaciones.
Fuente: Autores.			

Cuadro 14. Impacto de Riesgo.

Valor	Criterio	Descripción
1	Insignificante	Si el evento llega a ocurrir, tendría consecuencias mínimas para la empresa.
2	Menor	Si el evento llega a ocurrir, tendría consecuencias bajas para la empresa.
3	Moderado	Si el evento llega a ocurrir, tendría consecuencias medianas para la empresa.
4	Mayor	Si el evento llega a ocurrir, tendría consecuencias altas para la empresa.
5	Catastrófico	Si el evento llega a ocurrir, tendría consecuencias desastrosas para la empresa.
Fuente: Autores.		

En el cuadro 15, se describen los criterios de valoración del riesgo para evaluar su criticidad de acuerdo con la siguiente ecuación:

Riesgo = Impacto * Probabilidad de Ocurrencia

Cuadro 15. Valoración del riesgo.

	Probabilidad de ocurrencia				
Impacto	**Raro**	**Improbable**	**Posible**	**Probable**	**Frecuente**
Insignificante	1	2	3	4	5
Menor	2	4	6	8	10
Moderado	3	6	9	12	15
Mayor	4	8	12	16	20
Catastrófico	5	10	15	20	25

Fuente: Autores. Tomado como referencia la norma ISO 27005 Anexo E.

A continuación, en el cuadro 16, se describe la matriz de riesgos en el que se valoran a las amenazas encontradas:

Cuadro 16. Matriz de Riesgo T&S COMP. Tecnología y Servicios S.A.S.

Identificación del riesgo					Análisis de riesgos		
ID riesgo	**Tipo de impacto**	**Tipo de activo**	**Fuente/causa de la amenaza**	**Vulnerabilidad**	**Probabilidad de ocurrencia**	**Impacto**	**Valor**
R1	Ambiental	Hardware	Polvo, corrosión	Susceptibilidad a la humedad, polvo y suciedad.	3	5	15
R2	Operativo		Error en el uso de las funciones	Ausencia de un eficiente control de cambios en la configuración.	1	3	3
R3	Operativo		Fallas en el suministro de servicios eléctricos	Susceptibilidad a las variaciones de voltaje.	3	3	9
R4	Ambiental		Fenómenos Climatológicos	Susceptibilidad a las variaciones de temperatura.	2	3	6
R5	Operativo		Robo de documentos	Almacenamiento sin seguridad.	3	4	12
R6	Operativo		Mal manejo del dispositivo	Utilización inapropiada de dispositivos.	3	3	9
R7	Operativo	Software	Funcionamiento incorrecto de los dispositivos	Desactualización de software	2	2	4
R8	Operativo		Uso no autorizado del dispositivo	Ausencia de bloqueo de equipo cuando se abandona la estación de trabajo.	3	3	9
R9	Operativo			Gestión deficiente de las contraseñas.	1	4	4

Cuadro 16. (Continuación)

Identificación del riesgo					Análisis de riesgos		
ID riesgo	**Tipo de impacto**	**Tipo de activo**	**Fuente/causa de la amenaza**	**Vulnerabilidad**	**Probabilidad de ocurrencia**	**Impacto**	**Valor**
R10	Operativo	Software	Manipulación con software o hardware	Descarga y uso no controlado de software.	2	4	8
R11	Operativo	Red	Falla de las comunicaciones internas y externas	Falla del canal principal.	4	5	20
R12	Operativo		Espionaje remoto	Arquitectura de red insegura.	3	3	9
R13	Estratégico	Personal	Incumplimiento en la disponibilidad del personal	Ausencia del personal.	4	4	16
R14	Estratégico		Abuso de derechos	Desconocimiento en seguridad de la información.	5	4	20
R15	Operativo			Uso incorrecto de software y hardware.	4	3	12
R16	Estratégico			Falta de conciencia en materia de seguridad de la información.	3	4	12
R17	Estratégico		Robo de dispositivos o documentos	Desactualización de inventario de activos de información.	3	4	12
R18	Legal			Ausencia de procedimiento formal para el registro de ingreso y retiro de personas externas.	4	4	16

Cuadro 16. (Continuación)

Identificación del riesgo					Análisis de riesgos		
ID riesgo	**Tipo de impacto**	**Tipo de activo**	**Fuente/causa de la amenaza**	**Vulnerabilidad**	**Probabilidad de ocurrencia**	**Impacto**	**Valor**
R19	Imagen / Reputación	Personal	Fuga de información por parte de un empleado de la compañía.	Pérdida de confidencialidad en las propuestas licitatorias entregados por un empleado a un tercero (competencia).	4	5	20
R20	Financiero		Manipulación incorrecta de los activos del contratante	Pérdida o daño de activos de propiedad del contratante por inadecuadas prácticas al momento de realizar mantenimiento por parte del funcionario que ejecuta la actividad.	3	4	12
R21	Operativo		Suplantación de información (Phishing) Datos procedentes de fuentes no fiables	Consulta en páginas web sobre términos de referencia en procesos licitatorios que puedan contener información falsa.	1	5	5
R22	Financiero		Pérdida de disponibilidad sobre información contractual de los	Pérdida de información contractual de los clientes accidental o provocado por parte de un empleado.	3	4	12

			clientes.				

Cuadro 16. (Continuación)

Identificación del riesgo					Análisis de riesgos		
ID riesgo	**Tipo de impacto**	**Tipo de activo**	**Fuente/causa de la amenaza**	**Vulnerabilidad**	**Probabilidad de ocurrencia**	**Impacto**	**Valor**
R23	Legal	Información	Violación de confidencialidad de la información de la compañía	Manejo indebido de información confidencial a la cual tienen acceso los empleados.	3	4	12
R24	Imagen / Reputación		Perdida de confidencialidad en la información de los clientes	Divulgación no autorizada sobre la información de los clientes, generando pérdida de confianza en la compañía y acciones legales contra la misma.	3	4	12
R25	Operativo		Borrado accidental o intencional de información sensible.	Eliminación accidental o intencional de archivos que puede producir afectación en el desarrollo operacional de la compañía.	4	4	16
R26	Operativo		Cambios no autorizados en datos almacenados.	Modificación en información confidencial que se realiza de manera no autorizada, intencional o	3	4	12

				accidentalmente.			
R27	Imagen / Reputación		Divulgación de información contractual de los clientes.	Pérdida de confidencialidad sobre información contractual de los clientes.	3	4	12

Cuadro 16. (Continuación)

Identificación del riesgo					Análisis de riesgos		
ID riesgo	**Tipo de impacto**	**Tipo de activo**	**Fuente/causa de la amenaza**	**Vulnerabilidad**	**Probabilidad de ocurrencia**	**Impacto**	**Valor**
R28	Operativo	Organización	Almacenamiento de contraseñas de inicio de sesión.	Conservar contraseñas de inicio de sesión en plataformas en las que se almacena información sensible.	2	4	8
R29	Operativo		Uso o divulgación de contraseñas.	Uso o divulgación de contraseñas inseguras como método de ataque para adquirir información confidencial.	3	4	12
R30	Estratégico		Abuso de derechos	Ausencia de controles para el manejo de la información personal.	3	4	12
R31	Estratégico			Ausencia de controles en caso de incidentes de seguridad de la	3	4	12

				información.			
R32	Estratégico			Ausencia de políticas sobre limpieza de escritorio.	1	1	1

Cuadro 16. (Continuación)

Identificación del riesgo					Análisis de riesgos		
ID riesgo	**Tipo de impacto**	**Tipo de activo**	**Fuente/causa de la amenaza**	**Vulnerabilidad**	**Probabilidad de ocurrencia**	**Impacto**	**Valor**
R33	Operativo	Organización	Negación de acciones.	Ausencia de asignación de responsabilidades en Seguridad de la Información.	4	4	16
R34	Estratégico		Fallas de dispositivo.	Ausencia de planes para la gestión de continuidad de negocio.	4	4	16
Fuente: Autores. De acuerdo a la información suministrada por T&S COMP.							

Una vez valorados los riesgos de acuerdo a cada amenaza encontrada en T&S COMP. Tecnología y Servicios S.A.S, en el cuadro 17 se establecen niveles de aceptación del riesgo de acuerdo a las categorías determinadas en la valoración del riesgo. Se toma como referencia la norma ISO 27005 Anexo E.

Cuadro 17. Nivel de aceptación del riesgo.

Nivel de aceptación	Valor
Inaceptable	15 – 25
Moderado	5 – 14
Aceptable	1 – 4
Fuente: Autores. Tomado como referencia la norma ISO 27005 Anexo E	

La alta gerencia de T&S COMP. Tecnología y Servicios S.A.S decidió tomar una acción frente a las zonas de riesgos inaceptables ya que se deben trabajar mediante planes de tratamiento de riesgo y los controles establecidos para mitigarlos y mejorar la seguridad de sus recursos.

De acuerdo a los niveles de aceptación del riesgo evaluados en el cuadro 17, se realiza la aceptación de riesgos de acuerdo a las amenazas analizadas en el cuadro 18, como se observa a continuación:

Cuadro 18. Aceptación de Riesgos T&S COMP. Tecnología y Servicios S.A.S

Identificación del riesgo				Análisis de riesgos		
ID riesgo	**Tipo de activo**	**Fuente/causa de la amenaza**	**Vulnerabilidad**	**Probabilidad de ocurrencia**	**Impacto**	**Nivel de aceptación**
R1	Hardware	Polvo, corrosión	Susceptibilidad a la humedad, polvo y suciedad.	Posible	Catastrófico	Inaceptable
R2		Error en el uso de las funciones	Ausencia de un eficiente control de cambios en la configuración.	Raro	Moderado	Aceptable
R3		Fallas en el suministro de servicios eléctricos	Susceptibilidad a las variaciones de voltaje.	Posible	Moderado	Moderado
R4		Fenómenos Climatológicos	Susceptibilidad a las variaciones de temperatura.	Improbable	Moderado	Moderado
R5		Robo de documentos	Almacenamiento sin seguridad.	Posible	Mayor	Moderado
R6		Mal manejo del dispositivo	Utilización inapropiada de dispositivos.	Posible	Moderado	Moderado
R7	Software	Funcionamiento incorrecto de los dispositivos	Desactualización de software.	Improbable	Menor	Aceptable
R8		Uso no autorizado del dispositivo	Ausencia de bloqueo de equipo cuando se abandona la estación de trabajo.	Posible	Moderado	Moderado
R9			Gestión deficiente de las contraseñas.	Raro	Mayor	Aceptable

Cuadro 18. (Continuación)

Identificación del riesgo				Análisis de riesgos		
ID riesgo	**Tipo de activo**	**Fuente/causa de la amenaza**	**Vulnerabilidad**	**Probabilidad de ocurrencia**	**Impacto**	**Nivel de aceptación**
R10	Software	Manipulación con software o hardware	Descarga y uso no controlado de software.	Improbable	Mayor	Moderado
R11	Red	Falla de las comunicaciones internas y externas	Falla del canal principal.	Probable	Catastrófico	Inaceptable
R12		Espionaje remoto	Arquitectura de red insegura.	Posible	Moderado	Moderado
R13	Personal	Incumplimiento en la disponibilidad del personal	Ausencia del personal.	Probable	Mayor	Inaceptable
R14		Abuso de derechos	Desconocimiento en seguridad de la información.	Frecuente	Mayor	Inaceptable
R15			Uso incorrecto de software y hardware	Probable	Moderado	Moderado
R16			Falta de conciencia en materia de seguridad de la información	Posible	Mayor	Moderado
R17		Robo de dispositivos o	Desactualización de inventario de activos de información	Posible	Mayor	Moderado

R18		documentos	Ausencia de procedimiento formal para el registro de ingreso y retiro de personas externas	Probable	Mayor	Inaceptable

Cuadro 18. (Continuación)

Identificación del riesgo				Análisis de riesgos		
ID riesgo	**Tipo de activo**	**Fuente/causa de la amenaza**	**Vulnerabilidad**	**Probabilidad de ocurrencia**	**Impacto**	**Nivel de aceptación**
R19	Personal	Fuga de información por parte de un empleado de la compañía.	Pérdida de confidencialidad en las propuestas licitatorias entregados por un empleado a un tercero (competencia).	Probable	Catastrófico	Inaceptable
R20		Manipulación incorrecta de los activos del contratante	Pérdida o daño de activos de propiedad del contratante por inadecuadas prácticas al momento de realizar mantenimiento por parte del funcionario que ejecuta la actividad.	Posible	Mayor	Moderado
R21		Suplantación de información (Phishing) Datos procedentes de fuentes no fiables	Consulta en páginas web sobre términos de referencia en procesos licitatorios que puedan contener información falsa.	Raro	Catastrófico	Moderado

R22		Pérdida de disponibilidad sobre información contractual de los clientes.	Pérdida de información contractual de los clientes accidental o provocado por parte de un empleado.	Posible	Mayor	Moderado

Cuadro 18. (Continuación)

Identificación del riesgo				Análisis de riesgos		
ID riesgo	**Tipo de activo**	**Fuente/causa de la amenaza**	**Vulnerabilidad**	**Probabilidad de ocurrencia**	**Impacto**	**Nivel de aceptación**
R23	Información	Violación de confidencialidad de la información de la compañía	Manejo indebido de información confidencial a la cual tienen acceso los empleados.	Posible	Mayor	Moderado
R24		Perdida de confidencialidad en la información de los clientes	Divulgación no autorizada sobre la información de los clientes, generando pérdida de confianza en la compañía y acciones legales contra la misma.	Posible	Mayor	Moderado
R25		Borrado accidental o intencional de información sensible.	Eliminación accidental o intencional de archivos que puede producir afectación en el desarrollo operacional de la compañía.	Probable	Mayor	Inaceptable
R26		Cambios no autorizados en datos almacenados.	Modificación en información confidencial que se realiza de manera no autorizada,	Posible	Mayor	Moderado

			intencional o accidentalmente.			
R27		Divulgación de información contractual de los clientes.	Pérdida de confidencialidad sobre información contractual de los clientes.	Posible	Mayor	Moderado

Cuadro 18. (Continuación)

Identificación del riesgo				Análisis de riesgos		
ID riesgo	**Tipo de activo**	**Fuente/causa de la amenaza**	**Vulnerabilidad**	**Probabilidad de ocurrencia**	**Impacto**	**Nivel de aceptación**
R28	Organización	Almacenamiento de contraseñas de inicio de sesión.	Conservar contraseñas de inicio de sesión en plataformas en las que se almacena información sensible.	Improbable	Mayor	Moderado
R29		Uso o divulgación de contraseñas.	Uso o divulgación de contraseñas inseguras como método de ataque para adquirir información confidencial.	Posible	Mayor	Moderado
R30		Abuso de derechos	Ausencia de controles para el manejo de la información personal.	Posible	Mayor	Moderado
R31			Ausencia de controles en caso de incidentes de seguridad de la información.	Posible	Mayor	Moderado

R32			Ausencia de políticas sobre limpieza de escritorio.	Raro	Insignificante	Aceptable
R33		Negación de acciones.	Ausencia de asignación de responsabilidades en Seguridad de la Información.	Probable	Mayor	Inaceptable
R34		Fallas de dispositivo.	Ausencia de planes para la gestión de continuidad de negocio.	Probable	Mayor	Inaceptable
Fuente: Autores. Aceptación de riesgos por parte de T&S COMP..						

8. PLAN DE TRATAMIENTO DE LOS RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN

Teniendo en cuenta los riesgos identificados anteriormente, en esta etapa, se realiza el plan de tratamiento de riesgos, que, por medio de la implementación de controles, se busca disminuir el impacto que puede generar la materialización del riesgo sobre la infraestructura informática y los sistemas donde se maneja información sensible, para asegurar la integridad, disponibilidad y confidencialidad de la información en T&S COMP. Tecnología y Servicios S.A.S. Para esto, se tienen en cuenta las siguientes medidas de tratamiento:

- Eliminar el riesgo: Tomar las medidas encaminadas para impedir su materialización.
- Mitigar el riesgo: Tomar las medidas para disminuir tanto la probabilidad (medidas de protección), como el impacto (medidas de protección).
- Transferir el riesgo: Reducir el riesgo a través del traspaso de las pérdidas, como en el caso de un contrato de seguros, donde existe un riesgo compartido.
- Aceptar el riesgo: Aceptar el riesgo tolerable, es decir el riesgo residual que aún se mantiene.[38]

La implementación de los controles, se realizó en base a la norma ISO 27001:2013 en su Anexo A, de acuerdo a sus objetivos de control y el manejo de buenas prácticas. Los riesgos que se deben tratar de inmediato son los que se encuentran como “Inaceptable”. Se sugiere que se realice una validación de los controles, que permita mantener el riesgo o mitigarlo, para facilitar la toma de decisiones, con un mínimo de recursos que genere algún costo adicional a la empresa. El cuadro del tratamiento de riesgos está compuesta por la siguiente información:

- ID del riesgo
- El tipo de activo
- La fuente o causa de la amenaza
- Vulnerabilidad
- Nivel de aceptación
- Opción de tratamiento
- Control de tratamiento

[38] DEPARTAMENTO NACIONAL DE PLANEACIÓN, Guía metodológica para la administración de riesgos del SGSI [online]. [Consultado 15 de febrero de 2017]. Disponible en: https://colaboracion.dnp.gov.co/CDT/DNP/SE-G02%20Gu%C3%ADa%20metodol%C3%B3gica%20para%20la%20admon%20de%20riesgos%20del%20SGSI.Pu.pdf?

El tratamiento de riesgos involucra un proceso para definir si los niveles de riesgo son tolerables. En caso de no ser tolerables, se evalúa un tratamiento para modificar riesgos e implementar controles. Teniendo en cuenta la información anterior, en el cuadro 19 se procede por cada riesgo, a establecer el control que debe implementarse para determinar la opción de tratamiento según sea el caso: eliminar, mitigar, transferir y aceptar el riesgo, asociando el control y a su vez una recomendación de tratamiento según el tipo de riesgo al cual la empresa se esté enfrentando y se vean comprometidos los objetivos de la empresa.

Cuadro 19. Plan de tratamiento de riesgos T&S COMP. Tecnología y Servicios S.A.S

Identificación del riesgo				Análisis de riesgos	Plan de tratamiento a los riesgos	
ID riesgo	**Tipo de activo**	**Fuente/causa de la amenaza**	**Vulnerabilidad**	**Nivel de aceptación**	**Opción de tratamiento**	**Control de tratamiento**
R1	Hardware	Polvo, corrosión	Susceptibilidad a la humedad, polvo y suciedad.	Inaceptable	Mitigar	Se asocia con la implementación del Objetivo de Control Seguridad Física y de Entorno, A11.2.1 Ubicación y protección de los equipos, de la norma ISO 27001:2013 Anexo A, Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado, los equipos deben estar ubicados en una zona donde no exista humedad, se debe realizar mantenimiento preventivo a los equipos para evitar que el polvo y la suciedad los dañe.
R2		Error en el uso de las funciones	Ausencia de un eficiente control de cambios en la configuración.	Aceptable	Aceptar	Se asocia con la implementación del Objetivo de Control Seguridad Física y de Entorno, A11.2.4 Mantenimiento de los equipos, de la norma ISO 27001:2013 Anexo A, los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas, se debe establecer control sobre el mantenimiento y actualización de los equipos para evitar que por falta de configuración no se realice correctamente el uso de los equipos.

Cuadro 19. (Continuación)

Identificación del riesgo				Análisis de riesgos	Plan de tratamiento a los riesgos	
ID riesgo	**Tipo de activo**	**Fuente/causa de la amenaza**	**Vulnerabilidad**	**Nivel de aceptación**	**Opción de tratamiento**	**Control de tratamiento**
R3	Hardware	Fallas en el suministro de servicios eléctricos	Susceptibilidad a las variaciones de voltaje.	Moderado	Mitigar	Se asocia con la implementación del Objetivo de Control Seguridad Física y de entorno, A11.2.2. Servicios de suministro, de la norma ISO 27001:2013 Anexo A, los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro, Mantener reguladores de voltaje para evitar, daño en los equipos.
R4		Fenómenos Climatológicos	Susceptibilidad a las variaciones de temperatura.	Moderado	Transferir	Se asocia con la implementación del Objetivo de Control Seguridad Física y de Entorno, A11.1.4. Protección contra amenazas externas y ambientales, de la norma ISO 27001:2013 Anexo A, se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes, se debe transferir el riesgo a una compañía de seguros, para que, en caso de algún fenómeno climatológico, el riesgo sea compartido y se controle por intermedio de los dos.

Cuadro 19. (Continuación)

Identificación del riesgo				Análisis de riesgos	Plan de tratamiento a los riesgos	
ID riesgo	**Tipo de activo**	**Fuente/causa de la amenaza**	**Vulnerabilidad**	**Nivel de aceptación**	**Opción de tratamiento**	**Control de tratamiento**
R5	Hardware	Robo de documentos	Almacenamiento sin seguridad.	Moderado	Mitigar	Se asocia con la implementación del Objetivo de Control Seguridad Física y de Entorno, A11.2.9. Política de escritorio limpio y pantalla limpia, de la norma ISO 27001:2013 Anexo A, se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información, evitando la pérdida de información.
R6		Mal manejo del dispositivo	Utilización inapropiada de dispositivos.	Moderado	Mitigar	Se asocia con la implementación del Objetivo de Control, Gestión de Activos, A8.1.3. Uso aceptable de los activos, de la norma ISO 27001:2013 Anexo A, se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información, por medio de políticas se debe establecer el uso adecuado de los activos asociados con el manejo de la información.

Cuadro 19. (Continuación)

Identificación del riesgo				Análisis de riesgos	Plan de tratamiento a los riesgos	
ID riesgo	**Tipo de activo**	**Fuente/causa de la amenaza**	**Vulnerabilidad**	**Nivel de aceptación**	**Opción de tratamiento**	**Control de tratamiento**
R7	Software	Funcionamiento incorrecto de los dispositivos	Desactualización de software	Aceptable	Aceptar	Se asocia con la implementación del Objetivo de Control, Adquisición, desarrollo y mantenimiento de sistemas, A14.1.1. Análisis y especificación de requisitos de seguridad de la información, de la norma ISO 27001:2013 Anexo A, en donde los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes, de acuerdo a los requisitos se debe mantener actualizados los software de todos los dispositivos asociados con el manejo de la información.
R8	Software	Uso no autorizado del dispositivo	Ausencia de bloqueo de equipo cuando se abandona la estación de trabajo	Moderado	Mitigar	Se asocia con la implementación del Objetivo de Control, Control de Acceso, A9.4.2. Procedimiento de ingreso seguro, de la norma ISO 27001:2013 Anexo A, cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro, se debe establecer en la política de control de acceso el bloqueo de los equipos, en ausencia de su estación de trabajo.

Cuadro 19. (Continuación)

Identificación del riesgo				Análisis de riesgos	Plan de tratamiento a los riesgos	
ID riesgo	**Tipo de activo**	**Fuente/causa de la amenaza**	**Vulnerabilidad**	**Nivel de aceptación**	**Opción de tratamiento**	**Control de tratamiento**
R9	Software	Uso no autorizado del dispositivo	Gestión deficiente de las contraseñas	Aceptable	Aceptar	Se asocia con la implementación del Objetivo de Control, Control de Acceso, A9.4.3. Sistema de gestión de contraseñas, de la norma ISO 27001:2013 Anexo A, los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas, se debe establecer un control en donde se verifique la calidad de las contraseñas, estas son responsabilidad de cada usuario y son intransferibles.
R10		Manipulación con software o hardware	Descarga y uso no controlado de software	Moderado	Mitigar	Se asocia con la implementación del Objetivo de Control, Seguridad de las Operaciones, A12.6.2. Restricciones sobre la instalación de software, de la norma ISO 27001:2013 Anexo A, Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios, en las políticas de seguridad de las operaciones, se debe restringir, por parte de los usuarios no autorizados, la descarga e instalación de software.

Cuadro 19. (Continuación)

Identificación del riesgo				Análisis de riesgos	Plan de tratamiento a los riesgos	
ID riesgo	**Tipo de activo**	**Fuente/causa de la amenaza**	**Vulnerabilidad**	**Nivel de aceptación**	**Opción de tratamiento**	**Control de tratamiento**
R11	Red	Falla de las comunicaciones internas y externas	Falla del canal principal	Inaceptable	Mitigar	Se asocia con la implementación del Objetivo de Control, Seguridad de las Comunicaciones, A13.1.2. Seguridad de los servicios de red, de la norma ISO 27001:2013 Anexo A, se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente, se debe revisar por parte del coordinador TI el funcionamiento adecuado de las redes y dar cumplimiento de la política de seguridad de las comunicaciones.

Cuadro 19. (Continuación)

Identificación del riesgo				Análisis de riesgos	Plan de tratamiento a los riesgos	
ID riesgo	**Tipo de activo**	**Fuente/causa de la amenaza**	**Vulnerabilidad**	**Nivel de aceptación**	**Opción de tratamiento**	**Control de tratamiento**
R12	Red	Espionaje remoto	Arquitectura de red insegura	Moderado	Mitigar	Se asocia con la implementación del Objetivo de Control, Seguridad Física y del Entorno, A11.2.3. Seguridad en el cableado, de la norma ISO 27001:2013 Anexo A, el cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño, el coordinador de TI debe realizar seguimiento y revisión periódica a la arquitectura de red, no deben existir puertas traseras, también se debe hacer capacitación del personal en equipos de seguridad (firewall) para la adecuada gestión de seguridad de la información de la infraestructura de red de la empresa y evitar ingresos no autorizados.

Cuadro 19. (Continuación)

Identificación del riesgo				Análisis de riesgos	Plan de tratamiento a los riesgos	
ID riesgo	**Tipo de activo**	**Fuente/causa de la amenaza**	**Vulnerabilidad**	**Nivel de aceptación**	**Opción de tratamiento**	**Control de tratamiento**
R13	Personal	Incumplimiento en la disponibilidad del personal	Ausencia del personal	Inaceptable	Mitigar	Se asocia con la implementación del Objetivo de Control, Seguridad de los Recursos Humanos, A7.2.1.Responsabilidades de la Dirección, de la norma ISO 27001:2013 Anexo A, la dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización, por parte de la dirección se debe realizar el seguimiento para que el personal cumpla con sus funciones y evitar inconvenientes por falta del mismo, adicional deben tener personal de apoyo para suplir las ausencias.

Cuadro 19. (Continuación)

Identificación del riesgo				Análisis de riesgos	Plan de tratamiento a los riesgos	
ID riesgo	**Tipo de activo**	**Fuente/causa de la amenaza**	**Vulnerabilidad**	**Nivel de aceptación**	**Opción de tratamiento**	**Control de tratamiento**
R14	Personal	Abuso de derechos	Desconocimiento en seguridad de la información	Inaceptable	Mitigar	Se asocia con la implementación del Objetivo de Control, Seguridad de los Recursos Humanos, A7.2.2. Toma de conciencia, educación y formación en la seguridad de la información, de la norma ISO 27001:2013 Anexo A, todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo, se deben realizar campañas de concientización orientadas por el coordinador de TI y realizar el seguimiento pertinente, para garantizar que el personal esté capacitado en temas de seguridad de la información.

Cuadro 19. (Continuación)

Identificación del riesgo				Análisis de riesgos	Plan de tratamiento a los riesgos	
ID riesgo	**Tipo de activo**	**Fuente/causa de la amenaza**	**Vulnerabilidad**	**Nivel de aceptación**	**Opción de tratamiento**	**Control de tratamiento**
R15	Personal	Abuso de derechos	Uso incorrecto de software y hardware	Moderado	Mitigar	Se asocia con la implementación del Objetivo de Control, Gestión de Activos, A8.1.3. Uso aceptable de los activos, de la norma ISO 27001:2013 Anexo A, se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información, se debe establecer un seguimiento por parte del coordinador TI, para que las reglas sean acatadas por todo el personal y evitar el uso incorrecto de los activos.

Cuadro 19. (Continuación)

Identificación del riesgo				Análisis de riesgos	Plan de tratamiento a los riesgos	
ID riesgo	**Tipo de activo**	**Fuente/causa de la amenaza**	**Vulnerabilidad**	**Nivel de aceptación**	**Opción de tratamiento**	**Control de tratamiento**
R16	Personal	Abuso de derechos	Falta de conciencia en materia de seguridad de la información	Moderado	Mitigar	Se asocia con la implementación del Objetivo de Control, Seguridad de los Recursos Humanos, A7.2.2. Toma de conciencia, educación y formación en la seguridad de la información, de la norma ISO 27001:2013 Anexo A, todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo, se deben realizar campañas de concientización orientadas por el coordinador de TI y la alta gerencia, para realizar el seguimiento pertinente, para garantizar que el personal esté capacitado en temas de seguridad de la información, convirtiendo esa falta de conciencia en fortaleza para la compañía.

Cuadro 19. (Continuación)

Identificación del riesgo				Análisis de riesgos	Plan de tratamiento a los riesgos	
ID riesgo	**Tipo de activo**	**Fuente/causa de la amenaza**	**Vulnerabilidad**	**Nivel de aceptación**	**Opción de tratamiento**	**Control de tratamiento**
R17	Personal	Robo de dispositivos o documentos	Desactualización de inventario de activos de información	Moderado	Mitigar	Se asocia con la implementación de los Objetivos de Control, Seguridad Física y del Entorno, A11.2.1. Ubicación y protección de los equipos y Gestión de Activos, A8.1.1 Inventario de activos , de la norma ISO 27001:2013 Anexo A, los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado, los equipos deben tener guaya para evitar el robos, deben permanecer bloqueados con la contraseña asignada a cada usuario, se debe implementar la política de escritorio limpio, para evitar la pérdida de información, además se debe mantener actualizado el inventario de activos para determinar que activo hace falta, y así evitar fuga de información.

Cuadro 19. (Continuación)

Identificación del riesgo				Análisis de riesgos	Plan de tratamiento a los riesgos	
ID riesgo	**Tipo de activo**	**Fuente/causa de la amenaza**	**Vulnerabilidad**	**Nivel de aceptación**	**Opción de tratamiento**	**Control de tratamiento**
R18	Personal	Robo de dispositivos o documentos	Ausencia de procedimiento formal para el registro de ingreso y retiro de personas externas	Inaceptable	Mitigar	Se asocia con la implementación de los Objetivos de Control, Seguridad Física y del Entorno, A11.1.1. Controles de acceso físicos, de la norma ISO 27001:2013 Anexo A, las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado, en la recepción se debe colocar una planilla, en donde se registe tanto el ingreso como la salida de personal externo a las instalaciones, donde se especifique la hora de entrada, nombres y documento de identidad, persona a quien visita, cada persona es responsable de su visitante, garantizando la confidencialidad de la información de la empresa.

Cuadro 19. (Continuación)

Identificación del riesgo				Análisis de riesgos	Plan de tratamiento a los riesgos	
ID riesgo	**Tipo de activo**	**Fuente/causa de la amenaza**	**Vulnerabilidad**	**Nivel de aceptación**	**Opción de tratamiento**	**Control de tratamiento**
R19	Personal	Fuga de información por parte de un empleado de la compañía.	Pérdida de confidencialidad en las propuestas licitatorias entregados por un empleado a un tercero (competencia).	Inaceptable	Mitigar	Se asocia con la implementación de los Objetivos de Control, Seguridad de las Comunicaciones, A13.2.4. Acuerdos de confidencialidad o de no divulgación y Seguridad de los Recursos Humanos A7,1, de la norma ISO 27001:2013 Anexo A, Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información, se debe establecer desde la contratación del personal los acuerdos de confidencialidad antes, durante y después de la terminación del contrato, en caso de que no se cumpla el acuerdo, tendrán sanciones legales.

Cuadro 19. (Continuación)

Identificación del riesgo	Análisis de riesgos	Plan de tratamiento a los riesgos

ID riesgo	Tipo de activo	Fuente/causa de la amenaza	Vulnerabilidad	Nivel de aceptación	Opción de tratamiento	Control de tratamiento
R20	Personal	Manipulación incorrecta de los activos del contratante	Pérdida o daño de activos de propiedad del contratante por inadecuadas prácticas al momento de realizar mantenimiento por parte del funcionario que ejecuta la actividad.	Moderado	Mitigar	Se asocia con la implementación de los Objetivos de Control, Gestión de Activos, A8.2.3. Manejo de Activos, de la norma ISO 27001:2013 Anexo A, Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización, en el caso de los activos de los clientes se deben manejar de la mejor forma, manteniendo su integridad, se deben establecer procedimientos correctivos según sea el caso, en cada labor realizada en sitio.

Cuadro 19. (Continuación)

Identificación del riesgo	Análisis de riesgos	Plan de tratamiento a los riesgos

ID riesgo	Tipo de activo	Fuente/causa de la amenaza	Vulnerabilidad	Nivel de aceptación	Opción de tratamiento	Control de tratamiento
R21	Personal	Suplantación de información (Phishing) Datos procedentes de fuentes no fiables	Consulta en páginas web sobre términos de referencia en procesos licitatorios que puedan contener información falsa.	Moderado	Mitigar	Se asocia con la implementación del Objetivo de Control, Adquisición, desarrollo y mantenimiento de sistemas, A14.1.2. Seguridad de servicios de las aplicaciones en redes públicas, de la norma ISO 27001:2013 Anexo A, la información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas, Se debe informar al personal acerca de las últimas técnicas de Phishing que se están utilizando, para que puedan identificar algo inusual al momento de consultar algún proceso y lo deben reportar al coordinador TI, para tomar las medidas necesarias para evitar filtraciones y robo de información.

Cuadro 19. (Continuación)

Identificación del riesgo	Análisis de riesgos	Plan de tratamiento a los riesgos

ID riesgo	Tipo de activo	Fuente/causa de la amenaza	Vulnerabilidad	Nivel de aceptación	Opción de tratamiento	Control de tratamiento
R22	Personal	Pérdida de disponibilidad sobre información contractual de los clientes.	Pérdida de información contractual de los clientes accidental o provocado por parte de un empleado.	Moderado	Mitigar	Se asocia con la implementación del Objetivo de Control, Seguridad de las Operaciones, A12.3.1. Respaldo de la información, de la norma ISO 27001:2013 Anexo A, Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas, se deben definir las responsabilidades del personal respecto a la realización de copias de seguridad, además es necesario establecer mecanismos para su protección, para mantener la confidencialidad, integridad y disponibilidad de la información.

Cuadro 19. (Continuación)

Identificación del riesgo				Análisis de riesgos	Plan de tratamiento a los riesgos	
ID riesgo	Tipo de activo	Fuente/causa de la amenaza	Vulnerabilidad	Nivel de aceptación	Opción de tratamiento	Control de tratamiento

Cuadro 19. (Continuación)

Identificación del riesgo				Análisis de riesgos	Plan de tratamiento a los riesgos	
ID riesgo	**Tipo de activo**	**Fuente/causa de la amenaza**	**Vulnerabilidad**	**Nivel de aceptación**	**Opción de tratamiento**	**Control de tratamiento**
R23	Información	Violación de confidencialidad de la información de la compañía	Manejo indebido de información confidencial a la cual tienen acceso los empleados.	Moderado	Mitigar	Se asocia con la implementación del Objetivo de Control, Seguridad de las comunicaciones, A13.2.4. Acuerdos de confidencialidad o de no divulgación , de la norma ISO 27001:2013 Anexo A, se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información, establecer políticas de acuerdos de confidencialidad, en donde los empleados se comprometan a no divulgar información confidencial de la empresa y manejar buenas practicas respecto al manejo de la información.

Cuadro 19. (Continuación)

Identificación del riesgo				Análisis de riesgos	Plan de tratamiento a los riesgos	
ID riesgo	**Tipo de activo**	**Fuente/causa de la amenaza**	**Vulnerabilidad**	**Nivel de aceptación**	**Opción de tratamiento**	**Control de tratamiento**
R24	Información	Perdida de confidencialidad en la información de los clientes	Divulgación no autorizada sobre la información de los clientes, generando pérdida de confianza en la compañía y acciones legales contra la misma.	Moderado	Mitigar	Se asocia con la implementación del Objetivo de Control, Cumplimiento, A18.1.5. Privacidad y protección de información de datos personales, de la norma ISO 27001:2013 Anexo A, se deben asegurar la privacidad y la protección de la información de datos personales, como se exige e la legislación y la reglamentación pertinentes, cuando sea aplicable, se debe estipular desde un comienzo en las ordenes de servicio, bajo la Ley de protección de datos personales 1581 de 2012, garantizando a los clientes el buen manejo de su información y a su vez garantizando confianza.
R25		Borrado accidental o intencional de información sensible.	Eliminación accidental o intencional de archivos que puede producir afectación en el desarrollo operacional de la compañía.	Inaceptable	Mitigar	Se asocia con la implementación del Objetivo de Control, Seguridad de las operaciones, A12.3.1. Respaldo de la información, de la norma ISO 27001:2013 Anexo A, se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas, estas copias de respaldo deben ser mensuales para garantizar, en caso de pérdida o borrado intencional, que la información no se pierda, para evitar la afectación en el desarrollo operacional de la compañía.

Cuadro 19. (Continuación)

Identificación del riesgo				Análisis de riesgos	Plan de tratamiento a los riesgos	
ID riesgo	**Tipo de activo**	**Fuente/causa de la amenaza**	**Vulnerabilidad**	**Nivel de aceptación**	**Opción de tratamiento**	**Control de tratamiento**
R26	Información	Cambios no autorizados en datos almacenados.	Modificación en información confidencial que se realiza de manera no autorizada, intencional o accidentalmente.	Moderado	Mitigar	Se asocia con la implementación de los Objetivos de Control, Seguridad de las operaciones, A12.1.2. Gestión de cambios y Control de acceso, A9.2.5. Revisión de los derechos de acceso de usuarios, de la norma ISO 27001:2013 Anexo A, se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información, la información, los propietarios de los activos de información son los responsables del manejo de la información y el buen uso que esta, deben tener una política de control de acceso, en donde se asignen permisos según sea el perfil, para evitar modificaciones no autorizadas a la información confidencial de la empresa.

Cuadro 19. (Continuación)

Identificación del riesgo				Análisis de riesgos	Plan de tratamiento a los riesgos	
ID riesgo	**Tipo de activo**	**Fuente/causa de la amenaza**	**Vulnerabilidad**	**Nivel de aceptación**	**Opción de tratamiento**	**Control de tratamiento**
R27	Información	Divulgación de información contractual de los clientes.	Pérdida de confidencialidad sobre información contractual de los clientes.	Moderado	Mitigar	Se asocia con la implementación de los Objetivos de Control, Seguridad de las comunicaciones, A13.2.4. Acuerdos de confidencialidad o de no divulgación y Cumplimiento, A18.1.5. Privacidad y protección de información de datos personales, de la norma ISO 27001:2013 Anexo A, se debe establecer políticas de acuerdos de confidencialidad, en donde los empleados se comprometan a no divulgar información confidencial de los clientes y manejar buenas practicas respecto al manejo de la información, garantizando el cumplimiento de las políticas por intermedio de la aplicación de la Ley de protección de datos personales.
R28	Organización	Almacenamiento de contraseñas de inicio de sesión.	Conservar contraseñas de inicio de sesión en plataformas en las que se almacena información sensible.	Moderado	Mitigar	Se asocia con la implementación de los Objetivos de Control, Control de acceso, A9.4.3. Sistema de gestión de contraseñas, y Criptografía, A10.1.1. Política sobre el uso de los controles criptográficos, de la norma ISO 27001:2013 Anexo A, se deben establecer políticas sobre el uso de los controles criptográficos para el almacenamiento de las contraseñas, además se debe asegurar la calidad de las contraseñas, para que sean

						confiables.

Cuadro 19. (Continuación)

Identificación del riesgo				Análisis de riesgos	Plan de tratamiento a los riesgos	
ID riesgo	**Tipo de activo**	**Fuente/causa de la amenaza**	**Vulnerabilidad**	**Nivel de aceptación**	**Opción de tratamiento**	**Control de tratamiento**
R29	Organización	Uso o divulgación de contraseñas.	Uso o divulgación de contraseñas inseguras como método de ataque para adquirir información confidencial.	Moderado	Mitigar	Se asocia con la implementación de los Objetivos de Control, Control de acceso, A9.4.2. Procedimiento de ingreso seguro, y A9.4.4. Uso de programas utilitarios privilegiados y A9.4.3. Sistema de gestión de contraseñas, de la norma ISO 27001:2013 Anexo A, se debe establecer políticas de control de acceso, en donde se plasme el ingreso seguro a los sistemas, es responsabilidad del usuario tener contraseñas complejas, no pueden ser transferibles y no se debe utilizar la misma contraseña en diferentes sistemas, también se deben restringir y controlar los programas que puedan anular el sistema.

R30		Abuso de derechos	Ausencia de controles para el manejo de la información personal.	Moderado	Mitigar	Se asocia con la implementación del Objetivo de Control, Cumplimiento, A18.1.5. Privacidad y protección de información de datos personales, de la norma ISO 27001:2013 Anexo A, se deben asegurar la privacidad y la protección de la información de datos personales, como se exige e la legislación y la reglamentación pertinentes, cuando sea aplicable, se debe estipular desde un comienzo en las ordenes de servicio, bajo la Ley de protección de datos personales 1581 de 2012, garantizando el buen manejo de la información.

Cuadro 19. (Continuación)

Identificación del riesgo				Análisis de riesgos	Plan de tratamiento a los riesgos	
ID riesgo	**Tipo de activo**	**Fuente/causa de la amenaza**	**Vulnerabilidad**	**Nivel de aceptación**	**Opción de tratamiento**	**Control de tratamiento**
R31	Organización	Abuso de derechos	Ausencia de controles en caso de incidentes de seguridad de la información.	Moderado	Mitigar	Se asocia con la implementación del Objetivo de Control, Gestión de incidentes de seguridad de la información, A16.1.1. Responsabilidades y procedimientos, de la norma ISO 27001:2013 Anexo A, se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información, se sugiere el desarrollo de un proceso disciplinario mediante el cual puedan tomarse acciones respecto

Identificación del riesgo				Análisis de riesgos	Plan de tratamiento a los riesgos	
ID riesgo	Tipo de activo	Fuente/causa de la amenaza	Vulnerabilidad	Nivel de aceptación	Opción de tratamiento	Control de tratamiento
						a comportamientos, actuaciones, modificación, omisiones u errores que representen un incidente de la seguridad de la información que pueda afectar los objetivos de la organización.

Cuadro 19. (Continuación)

Identificación del riesgo				Análisis de riesgos	Plan de tratamiento a los riesgos	
ID riesgo	Tipo de activo	Fuente/causa de la amenaza	Vulnerabilidad	Nivel de aceptación	Opción de tratamiento	Control de tratamiento

R32	Organización	Abuso de derechos	Ausencia de políticas sobre limpieza de escritorio.	Aceptable	Aceptar	Se asocia con la implementación del Objetivo de Control, Seguridad física y del entorno, A11.2.9. Política de escritorio limpio y pantalla limpia, de la norma ISO 27001:2013 Anexo A, Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información, se debe definir una política en donde tanto los documentos físicos y lógicos, que sean vitales y confidenciales para la empresa, sean almacenados de forma segura para evitar el acceso no autorizado por parte de un tercero, los documentos físicos deben ser almacenados bajo llave y no deben estar al alcance de personas ajenas al negocio.

Cuadro 19. (Continuación)

Identificación del riesgo				Análisis de riesgos	Plan de tratamiento a los riesgos	
ID riesgo	**Tipo de activo**	**Fuente/causa de la amenaza**	**Vulnerabilidad**	**Nivel de aceptación**	**Opción de tratamiento**	**Control de tratamiento**

R33	Organización	Negación de acciones.	Ausencia de asignación de responsabilidades en Seguridad de la Información.	Inaceptable	Mitigar	Se asocia con la implementación del Objetivo de Control, Organización de la seguridad de la información, A6.1.1. Roles y responsabilidades para la seguridad de la información, de la norma ISO 27001:2013 Anexo A, Se deben determinar los roles y las responsabilidades que el oficial de la seguridad de la información debe tener frente a la organización, informando a la alta gerencia el desempeño que tenga el sistema de gestión de la seguridad de la información. Así mismo, se establecen los roles y responsabilidades que debe tener todo el personal de la organización respecto a la seguridad de la información.

Cuadro 19. (Continuación)

Identificación del riesgo				Análisis de riesgos	Plan de tratamiento a los riesgos	
ID riesgo	**Tipo de activo**	**Fuente/causa de la amenaza**	**Vulnerabilidad**	**Nivel de aceptación**	**Opción de tratamiento**	**Control de tratamiento**

R34	Organización	Fallas de dispositivo.	Ausencia de planes para la gestión de continuidad de negocio.	Inaceptable	Mitigar	Se asocia con la implementación del Objetivo de Control, Aspectos de seguridad de la información de la gestión, A17.1.1. Planificación de la continuidad de la seguridad de la información , de la norma ISO 27001:2013 Anexo A, la organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre, Se deben identificar los riesgos, establecer los procedimientos y mecanismos para preservar la seguridad de los equipos de cómputo y servidores, proteger la información almacenada en ellos, y garantizar la continuidad de las funciones de la empresa T&S COMP Tecnología y Servicios S.A.S.
Fuente: Autores. De acuerdo a la información encontrada en el proceso de evaluación de riesgos.						

9. POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Las políticas y controles de seguridad surgen de la necesidad de proteger los activos fundamentales de información y, como herramienta sustancial, para concientizar a los colaboradores sobre su importancia, permitiendo a la empresa mantenerse en un ambiente competitivo. Por esto, se debe planificar adecuadamente controles de seguridad en la organización asegurando la integridad, disponibilidad y confidencialidad de la información.

9.1 POLÍTICA Y ALCANCE DEL SGSI

T&S COMP. Tecnología y Servicios S.A.S, consciente del gran valor de implementar un ambiente seguro, establece el propósito de implantar un modelo que permita identificar y mitigar los riesgos a los que está expuesta su información. Ante esta situación, se define la política general para garantizar la protección de sus activos, generando una estrategia orientada a una cultura de ciberseguridad.

El alcance de la política general de Seguridad de la Información de la compañía aplica a todos los recursos, dependencias, procesos internos y externos, servicios, funcionarios, proveedores y clientes, para asegurar adecuadamente los sistemas tecnológicos de T&S COMP. Tecnología y Servicios S.A.S.

En la política general de la empresa T&S COMP. Tecnología y Servicios S.A.S., con código PSG-01, se especifica el plan del SGSI de acuerdo al propósito de la empresa, los objetivos de seguridad de la Información para su establecimiento y el compromiso de mejora continua. Todo esto realizado conforme a los requisitos legales y contractuales, y acorde a la misión y visión de la entidad.

La política general de se describe de la siguiente forma:

> *"T&S COMP. Tecnología y servicios S.A.S. consciente de la importancia de la Seguridad de la Información, se ha comprometido con el establecimiento, implementación, operación y mejoramiento del Sistema de Gestión de Seguridad de la Información (SGSI) con el propósito de garantizar la confidencialidad, integridad y disponibilidad de los activos de información, que soportan los procesos de la organización, buscando reducir el impacto que generan las amenazas identificadas y acorde con las necesidades de las áreas interesadas (funcionarios, clientes, proveedores).*
>
> *La presente política se establece conforme al estricto cumplimiento de los requisitos legales y en concordancia con la misión y visión de la entidad.*

La política general de Seguridad de la Información de T&S COMP. Tecnología y servicios S.A.S, se encuentra soportada por políticas y procedimientos para garantizar el manejo adecuado de la información en la organización."

Para establecer la Política General de Seguridad de la Información de la empresa T&S COMP. Tecnología y Servicios S.A.S, se tomó como referencia la guía del Modelo de Seguridad para la elaboración de la política general de seguridad y privacidad de la información del Ministerio de Tecnologías de la Información y las Comunicaciones, y basados en la norma ISO/IEC 27001:2013.

9.1.1 Objetivos de seguridad de la información. T&S COMP. Tecnología y servicios S.A.S consciente del gran valor de implementar un ambiente seguro, incluye los objetivos de Seguridad de la Información:

- Cumplir con los principios y ser coherentes con la política de Seguridad de la Información.
- Evaluar los riesgos identificados en los activos de Información de los procesos de la organización.
- Realizar la valoración de los riesgos de acuerdo a los requisitos de seguridad aplicables, los resultados de evaluación y el tratamiento de riesgos.
- Fortalecer la cultura de Seguridad de la Información.
- Comunicar y actualizar políticas y procedimientos de Seguridad de la Información.
- Generar confianza a los funcionarios, proveedores, clientes y terceros en materia de Seguridad de la Información.
- Verificar la efectividad del Sistema de Gestión de Seguridad de la Información.
- Mejorar y realizar acciones preventivas y correctivas para el Sistema de Gestión de la Información.
- Garantizar la continuidad de negocio frente a incidentes.

9.2 ROLES Y RESPONSABILIDADES EN LA ORGANIZACIÓN

9.2.1 Alta gerencia.

- Tiene la responsabilidad de verificar y aprobar el Sistema de Gestión de Seguridad de la Información (SGSI).
- Realizar seguimiento al cumplimiento de las políticas de seguridad de la información, mensualmente.

- Apoyar la divulgación y aprobación del cumplimiento del Sistema de Gestión de Seguridad de la Información, enfocándose en los controles que aplican para cada caso.
- Establecer un monitoreo anual, en donde se realice auditoría a todo el sistema de seguridad de la información, para determinar que amenazas existen y mitigarlas.
- Tratar la Seguridad de la Información, con prioridad alta, para generar un ambiente de seguridad positivo, fomentando las buenas prácticas.

9.2.2 Funcionario responsable de la Seguridad de la Información.

- Tiene la responsabilidad de dar cumplimiento de las políticas y controles de seguridad de la información.
- Reportar a la alta gerencia el funcionamiento del Sistema de Gestión de seguridad de la información.
- Documentar y monitorear todos los incidentes de seguridad de la información.
- Preservar la Confidencialidad, Integridad y Disponibilidad, de la información y su infraestructura informática.

9.2.3 Funcionarios.

- Reportar cualquier incidente de seguridad de la información al director de TI.
- Dar cumplimiento a las políticas de seguridad de la información establecidas por la empresa.
- Entender y aplicar los programas de concientización establecidos por el área de TI, respecto a la seguridad de la información y el uso de las buenas practicas.

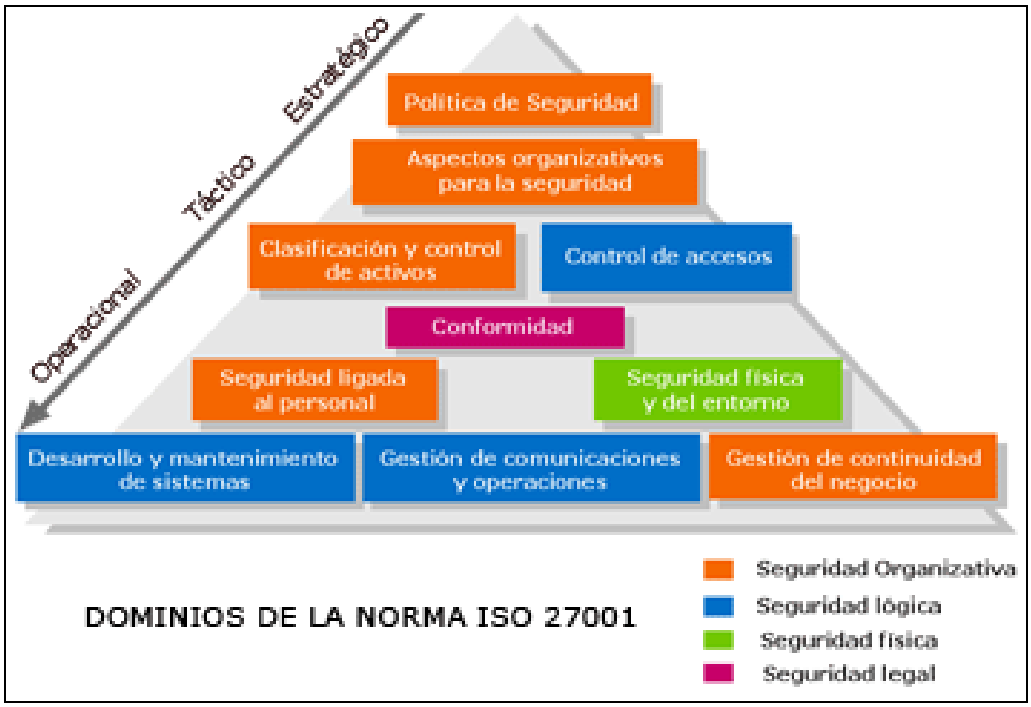
9.3 DOMINIOS DE LA NORMA ISO 27001:2013

Teniendo en cuenta el tratamiento de los riesgos, previamente establecido, se determinan los planes y recomendaciones para el cumplimiento de los controles del Anexo A de la Norma ISO 27001:2013, en base a sus 14 dominios, 35 objetivos de control y sus 114 controles de seguridad.

En la figura 6, se exponen los dominios de la norma: los dominios estratégicos, conformados por las políticas de seguridad y aspectos organizativos para la seguridad que ayudan a la organización a generar lineamientos conforme a los requisitos legales, a implementar y vigilar la Seguridad de la Información. Los dominios tácticos, conformados por clasificación de activos y control de acceso favorece a salvaguardas los recursos de Seguridad de la Información de la entidad; y los dominios operacionales, conformados por conformidad, seguridad del personal, seguridad física y del entorno, desarrollo y mantenimiento de

sistemas, gestión de comunicaciones y operaciones, y gestión de continuidad del negocio ayudan a garantizar la Seguridad de la Información en la entidad.

Figura 6: Dominios ISO 27001:2013



Fuente: TCPSI[39]

De acuerdo a los resultados, respecto a los controles, se efectúo un análisis a partir de los hallazgos encontrados y se establecen a su vez las políticas según cada objetivo de control, los cuales se explican a continuación:

9.3.1 Políticas de la Seguridad de la Información A5. El objetivo de control no se cumple del todo, teniendo en cuenta que tienen unas políticas definidas y socializadas, pero no les realizan el seguimiento, teniendo como consecuencias el incumplimiento por parte de los empleados, proveedores y clientes, de sus obligaciones interpuestas en las políticas de seguridad.

Al no realizar la revisión de las políticas, no se actualizan y, por consiguiente, no se sabe que cambios ha tenido desde su divulgación, perdiendo su conveniencia, adecuación y eficacia continua.

Se recomendó actualizar las políticas existentes, y realizar una verificación de lo que se está cumpliendo, con el fin de mantener eficacia continua.

[39] TCPSI. Dominios de la norma ISO 27001:2013 [Online]. [Consultado 21 de enero de 2017]. Disponible en: http://www.tcpsi.com/vermas/iso_27001.htm

Por lo tanto, desde la Alta Gerencia, los empleados, proveedores y clientes deben cumplir con las políticas de Seguridad de la Información, establecidas en el documento, mediante la implementación de buenas prácticas en la gestión de riesgos, el buen manejo de los activos de información, garantizando la Confidencialidad, Integridad y Disponibilidad de la información.

Las políticas de seguridad de la información en la empresa T&S COMP. Tecnología y Servicios S.A.S, se deberán revisar con una frecuencia mínima de dos veces al año, o antes si se producen cambios significativos. Todo cambio debe ir autorizado por la Alta Gerencia, y asesorado por el departamento de sistemas, específicamente por el Coordinador IT y en colaboración con los líderes de Gestión de Calidad y Recursos Humanos. El encargado de las revisiones es el Coordinador IT que reportará alguna falla o incumplimiento de las políticas de seguridad de la información a la Alta Gerencia.

9.3.2 Organización de la seguridad de la información A6. Teniendo en cuenta que es una empresa pequeña, está designado el Coordinador de TI, quien tiene la responsabilidad de velar por la seguridad de la información, junto con los interesados (usuarios, Proveedores y clientes), quienes son los que están involucrados en los procesos de la empresa, definiendo los roles y responsabilidades de la seguridad de la información.

Teniendo en cuenta que la empresa T&S COMP. Tecnología y Servicios S.A.S, no está regida por una entidad específica, y al trabajar con el estado en sus proyectos, les exigen algunas normas como:

- Ley de protección de datos personales 1581 de 2012[40]
- Ley 527 de 1999[41]

Por otro lado, al revisar si tienen contacto con grupos de interés especial, la empresa cuenta con una asesoría externa, por parte de una persona natural, quien los asesora provisionalmente para cumplir con los requisitos de la seguridad de la información, no cuentan con otro tipo de asesoría por parte de una empresa especializada en seguridad informática.

En cuanto al teletrabajo, no se encuentra implementado en la empresa, por lo tanto no aplica.

[40] ALCALDIA MAYOR DE BOGOTA. Ley Estatutaria 1581 de 2012 [Online]. [Consultado 20 de diciembre de 2016]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

[41] ALCALDIA MAYOR DE BOGOTA. Ley 527 de 1999 [Online]. [Consultado 31 de enero de 2016]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276

El Coordinador IT será el encargado de supervisar el cumplimiento de las políticas de Seguridad de la Información, junto con la Alta Gerencia. En caso que alguna área solicite asesoría al respecto, él dará dicha asesoría. Por esta razón, se deben tener en cuenta las siguientes políticas:

Todos los empleados y contratistas que desempeñen sus funciones en la empresa T&S COMP. Tecnología y Servicios S.A.S, tendrán acceso solo a la información necesaria para el desarrollo de sus funciones. En caso que una persona externa a la empresa solicite acceso a la información, debe justificar la labor a realizar para limitar el acceso a la información que necesite y con la autorización del líder de proceso con previo aviso al Coordinador IT.

Se deberán revisar semestralmente los acuerdos de confidencialidad y no divulgación de la información establecidos desde un comienzo para verificar que efectivamente se esté cumpliendo.

Política de uso de dispositivos para movilidad: El uso de los equipos portátiles y/o dispositivos extraíbles fuera de las instalaciones de la empresa T&S COMP. Tecnología y Servicios S.A.S únicamente se permitirá a usuarios autorizados por el departamento de Sistemas y la Alta Gerencia con previa solicitud de la dependencia respectiva, por medio de un acta de salida en donde se relacionen las características de los equipos y el responsable del mismo. Se protegerán mediante el uso de los siguientes controles tecnológicos:

- Cifrado de datos
- Restricción en la ejecución de aplicaciones propias de la Empresa.
- Restricción de conexión a la Red LAN de la empresa.
- Restricción de conexiones remotas.
- Protección física mediante guaya de seguridad.

Se realizará seguimiento a los roles y responsabilidades que cada persona de la empresa debe cumplir, para dar acatamiento a las políticas de la organización y establecer un contacto directo con las autoridades pertinentes a la seguridad de la información y con los grupos de interés.

9.3.3 Seguridad de los recursos humanos A7. Antes de asumir el empleo, se realiza la revisión de antecedentes judiciales, disciplinarios y fiscales, y en algunos casos visita domiciliaria.

Se establece en el contrato el acuerdo de confidencialidad y buen manejo de la información. En los acuerdos contractuales con los empleados y los contratistas se deberán establecer los roles y responsabilidades determinadas por la empresa

T&S COMP. Tecnología y Servicios S.A.S, en cumplimiento con la presente Política de Seguridad de la Información.

Durante la ejecución del empleo, no se lleva un seguimiento por parte de la alta gerencia, solo es de palabra y no está documentada. De acuerdo a las charlas de concientización a los empleados, se les explica la importancia de la seguridad de la información en cada una de sus labores, como tener buenas prácticas para el desarrollo de sus actividades y así poder cumplir con las políticas de seguridad de la información establecidas por la empresa. En el momento, no se cumple lo explicado, ya que la mayoría de empleados no le dan la importancia que debe tener la seguridad de la información.

Durante la ejecución del empleo, se deben realizar capacitaciones en Seguridad de la Información periódicamente y de forma obligatoria, para todo el personal y para quienes se vinculen de manera temporal y/o indefinida. Esta información se dará en las inducciones y debe estar documentada.

Todos los empleados y contratistas tendrán acceso a las políticas de Seguridad de la Información para su acatamiento, publicadas previamente, y se establecerá un documento de compromiso firmado para el cumplimiento de la política ya conocida.

El Departamento de Sistemas, en cabeza del Coordinador IT, realizará capacitaciones de sensibilización a todos los empleados y contratistas de la empresa T&S COMP. Tecnología y Servicios S.A.S de las actualizaciones periódicas en las políticas y procedimientos de la organización, que sea relevante para cada uno de los cargos, y según sea su rol dentro de la empresa.

Cuando un empleado cometa una violación de Seguridad de la Información, se iniciará un proceso disciplinario formal. Se le dará a conocer el llamado de atención para evitar tomar medidas en contra del empleado, y deberá justificar la razón del error cometido y asumir las consecuencias.

En la terminación y cambio de empleo, se establece en el contrato inicial, el acuerdo de confidencialidad tanto durante la ejecución del empleo, como la terminación del mismo.

Es responsabilidad del área de talento humano y del departamento de sistemas asegurar que en el evento de la terminación y/o cambio de cargo al interior de T&S COMP. Tecnología y Servicios S.A.S, el usuario debe hacer la devolución de todos los activos de información y elementos asignados durante su relación, mediante un acta de entrega firmada por las partes.

La vigencia de los derechos de acceso y su revocatoria, debe estar estrechamente relacionados con la terminación de la relación laboral y/o contractual.

Se recomienda, por parte de la alta gerencia exigir a todos los empleados y contratistas la aplicación de la seguridad de la información, llevando documentado el seguimiento al cumplimiento de las políticas de seguridad de la información.

9.3.4 Gestión de activos A8. Responsabilidad por los activos: tienen un inventario de los activos físicos de la empresa, y de algunos activos de información, sin embargo, no está actualizado, teniendo varios activos que ya no están en uso y que ya no son vitales para la empresa.

Todos los activos de información en la empresa T&S COMP. Tecnología y Servicios S.A.S, serán clasificados según el proceso al que pertenece y su contenido. Los controles adecuados serán implementados de acuerdo a su importancia en la empresa y en la de los clientes. También serán asignados propietarios a cada activo, el cual será responsable por el buen uso de ellos. El inventario de activos debe permanecer actualizado por lo menos una vez al año. Esta labor debe estar a cargo del Coordinador IT, apoyado por los líderes de procesos de las diferentes áreas.

Para la devolución de los activos, todos los empleados y contratistas deberán devolver todos los activos de la organización en su poder a la terminación de su empleo, mediante acta de entrega firmada y se deberá generar el paz y salvo de ello.

En la empresa T&S COMP. Tecnología y Servicios S.A.S no manejan una clasificación e identificación de los activos, además el inventario esta desactualizado y, por lo tanto, no permite conocer el nivel de criticidad de la información de acuerdo a la Confidencialidad, Integridad y Disponibilidad.

Por esto, se debe cumplir con la clasificación de los activos según el proceso y su contenido. Esta clasificación debe ser realizada por el responsable de cada proceso en apoyo de las personas a su cargo, teniendo en cuenta su valor relativo, su privacidad, sensibilidad, el nivel de riesgo al que se está expuesto y los requerimientos legales según sea el caso.

Las aplicaciones de los controles se utilizan para proveer un nivel de protección de la Información apropiado y consistente dentro de la organización, sin importar el medio, formato o lugar donde se encuentren. Estos controles se aplican y mantienen durante el ciclo de vida de la Información, desde su creación, durante su uso autorizado y hasta su apropiada disposición o destrucción.

Cuando la información clasificada de la empresa T&S COMP. Tecnología y Servicios S.A.S o de sus clientes, deba ser entregada a contratistas o terceros involucrados en el negocio, se deben firmar acuerdos de confidencialidad y no

divulgación de la información. Esta labor debe estar supervisada por el Coordinador IT, apoyado por la Alta Gerencia.

Para el acceso a información secreta confidencial y restringida, las terceras partes que requieran acceso a información en medio físico y/o electrónico, deben presentar a T&S COMP. Tecnología y Servicios S.A.S una autorización por parte de la Alta Gerencia y se debe firmar un acuerdo de confidencialidad indicando las restricciones de uso de dicha información. Se deben utilizar los mecanismos apropiados de control de acceso a la información dependiendo de su nivel de clasificación, los contratistas, pasantes o estudiantes no pueden tomar información secreta, confidencial y/o restringida cuando termine su vínculo con la empresa.

Para el manejo de medios, se establecieron restricciones sobre los medios removibles, bloqueando los puertos de las terminales de trabajo de los empleados de T&S COMP. Tecnología y Servicios S.A.S. Los equipos que tienen autorizado el manejo de USB y unidades CD/DVD deben tener las siguientes especificaciones: habilitado el escaneo automático de virus y tener configurada la herramienta de antivirus corporativo para evitar la reproducción automática de archivos ejecutables. También se debe proteger la información en su transferencia para evitar el acceso no autorizado y garantizar su Integridad. Para los dispositivos que hacen parte de la empresa que están en desuso, se realiza un acta de entrega del mismo.

Se recomienda actualizar los inventarios de los activos de información, clasificándolos e identificándolos, según su Confidencialidad, Integridad y Disponibilidad para determinar su nivel de criticidad.

9.3.5 Control de acceso A9. En los requisitos del negocio para el control de acceso se cumplen con las políticas de control de acceso. Todos los empleados deben registrar su entrada en una planilla y a su vez de las personas que son externas a las instalaciones. Cada empleado es responsable de la persona externa que lo acompaña. En cuanto al acceso a las redes y servicios, están restringidos los ingresos a determinados sitios en todas las terminales de la empresa T&S COMP. Tecnología y Servicios S.A.S. Adicionalmente, el uso del Wifi es restringido y para uso de los empleados. Cuando un externo solicita el acceso debe enviar un correo explicando la razón por la cual solicita el acceso y solo así se le otorga el permiso de ingreso bajo normas de seguridad para evitar que exista robo de información.

Se debe tener en cuenta la siguiente política de control de acceso:

Garantizar entornos con controles de acceso idóneos, los cuales aseguran el perímetro, tanto en Datacenter, oficinas, recintos, áreas de carga y descarga, así como en entornos abiertos para evitar el acceso no autorizado a ellos. Del mismo

modo, controlar las amenazas físicas externas y velar por proveer las condiciones medioambientales requeridas para el funcionamiento de la plataforma tecnológica y para la preservación de sus activos de información.

Así mismo, se debe exigir a los proveedores de servicios de tecnología, el cumplimiento de la implantación y efectividad de mecanismos de seguridad física, controles de acceso físico y condiciones medioambientales con que éste debe contar.

Los empleados responsables de las áreas seguras tienen la obligación de vigilar y garantizar que se cumplan las siguientes medidas de seguridad:

- El acceso a áreas seguras donde se procesa o almacena información top Secret, confidencial y restringida es limitado únicamente a personas autorizadas.
- Los accesos a áreas seguras requieren esquemas de control de acceso como tarjetas, llaves o candados.
- El responsable de un área segura debe garantizar que no ingresen cámaras fotográficas, videos, teléfonos móviles con cámaras, salvo se tenga una autorización expresa del departamento de sistemas.
- Se utilizan planillas para registrar la entrada y salida del personal.
- Se restringe el acceso físico a dispositivos como: puntos de acceso inalámbricos, puertas de enlace a redes y terminales de red que estén ubicadas en las áreas seguras.

La gestión de acceso a usuarios se maneja con perfiles para el ingreso de los usuarios, no todos los empleados tienen los mismos privilegios, los únicos que tienen acceso a todo es la alta gerencia y la dirección de tecnología. Se deberán llevar procesos formales para el registro y anulación de permisos de acceso a los usuarios. Esta labor está a cargo del Coordinador IT.

Se debe identificar y autenticar a cualquier usuario que, de manera local o remota, requiera utilizar los recursos de tecnología y operación de T&S COMP. Tecnología y Servicios S.A.S., para lo que se requiere contar con sistemas de seguridad que cumplan con las siguientes características:

- Debe estar activo para acceder a la plataforma tecnológica y de operación de T&S COMP. Tecnología y Servicios S.A.S., lo que significa que cada usuario tiene que identificarse y autenticarse antes de acceder a un recurso de tecnología por medio de un usuario y una contraseña.
- Los eventos de ingreso y autenticación de usuarios serán registrados y monitoreados por los responsables de la información.

El responsable de la información es el único que puede autorizar la creación de un usuario, este identificador de usuario debe ser asociado sólo a un individuo y la solicitud debe obedecer a una razón legítima de negocio. Por otro lado, los propietarios de los activos deben revisar los derechos de acceso de los usuarios mínimo una vez por semana, cualquier irregularidad se tomará como un incidente de Seguridad de la Información.
Responsabilidad de los usuarios, cada usuario es responsable de su autenticación y de lo que se realice con su perfil, se deben cumplir buenas prácticas para el uso de la información, es difícil que los empleados cumplan con las políticas de contraseñas y de usuarios, todo debe ir documentado y debe estar al alcance de los empleados, para que ellos hagan uso correcto de sus perfiles y roles.

Control de acceso a sistemas y aplicaciones, los empleados tienen asignados los roles y permisos para los accesos a los sistemas, sin embargo, si en el sistema se realizan cambios, es necesario retirar o asignar permisos según sea el caso. Para la gestión de contraseñas, cada usuario recibirá una clave o contraseña para acceder a los recursos informáticos de la empresa T&S COMP. Tecnología y Servicios S.A.S, esta contraseña debe ser cambiada de inmediato al primer ingreso, garantizando así la responsabilidad del usuario en su divulgación, la contraseña debe tener una longitud mínima de ocho caracteres alfanuméricos, diferentes a nombre propios o cualquier palabra de fácil acceso, se recomienda el cambio de las claves con una periodicidad de 60 días, esta labor está a cargo de cada usuario, pero estará supervisada por el Coordinador IT.

En cuanto a las restricciones para los códigos fuente, no es necesario teniendo en cuenta que en la empresa T&S COMP. Tecnología y Servicios S.A.S, no realizan desarrollos de software, todos sus aplicativos son contratados por terceros.

Se recomienda implementar la política de control de acceso definida anteriormente, en donde se verifique la calidad de las contraseñas, estas son responsabilidad de cada usuario y son intransferibles, se verifiquen los roles asignados a cada uno de los perfiles y realizan seguimiento a los perfiles con más privilegios para evitar incidentes de seguridad de la información.

9.3.6 Criptografía A10. Son implementados los controles criptográficos, para los discos de réplica en tiempo real del histórico de la información, el cual se realiza semanalmente, de esta manera se garantiza que la información está segura ante cualquier eventualidad que se pueda presentar, teniendo un respaldo de la misma, garantizando la continuidad del negocio.

La política sobre uso, protección y duración de las claves criptográficas se realiza a través del directorio activo durante todo su ciclo de vida.

Se recomienda cumplir con la implementación de los controles criptográficos, en donde se encuentre la información vital de la empresa, con accesos restringidos, y asignados al coordinador IT, quien será el responsable de realizar el seguimiento al cumplimento de los controles.

9.3.7 Seguridad física y del entorno A11. Áreas seguras en las instalaciones de T&S COMP. Tecnología y Servicios S.A.S, no cuentan con áreas de acceso restringido, la única parte que tiene el acceso restringido es el datacenter, el cual tiene acceso biométrico, solo para el coordinador IT y la alta gerencia. Para la seguridad física de las instalaciones, cuentan con CCTV y empresa de monitoreo, donde tiene sensores de movimiento y en caso de que el personal deba quedarse después de sus jornadas laboras comunes, deben informar con tiempo a la empresa de monitoreo, para que ellos les den el permiso y estén al tanto de los movimientos de los empleados. En caso de que se activen las alarmas, la empresa de monitoreo maneja el protocolo de seguridad el cual consiste en realizar llamadas a los celulares autorizados para verificar si existe alguna actividad inicial, sin embargo, envían a un motorizado para que verifique el sitio y emita un reporte.

Se garantizarán áreas seguras por medio de controles de entrada idóneos, que permitan el acceso únicamente al personal autorizado. Cuando se realiza el ingreso a un tercero, este se debe registrar en una bitácora ubicada en un lugar visible a la entrada de las instalaciones, indicando el área a la cual se dirige y el empleado a cargo de esta persona. También se debe registrar la hora de ingreso y la hora de salida, y si ingresa algún medio portátil.

Cuando los empleados se levanten de sus puestos de trabajo, es indispensable el bloqueo de los equipos, para evitar el ingreso no autorizado a sus estaciones de trabajo y así se pueda perder información vital de la empresa.

Todos los empleados en las instalaciones de la empresa o cuando prestan sus servicios donde un cliente deben permanecer con el carnet que los identifica como empleados y/o contratistas de T&S COMP. Tecnología y Servicios S.A.S y su uniforme o chaleco con los distintivos de la compañía, mientras permanezcan en las instalaciones.

La documentación física generada, recibida y, en general, manipulada por los empleados de la empresa y los empleados provistos por terceras partes deben estar ubicada en archivos o repositorios con condiciones de temperatura y humedad adecuadas, de acuerdo con las directrices de la función archivística de la empresa.

Equipos, el mecanismo para el control de acceso a los equipos, se maneja por intermedio de contraseñas asignadas a cada usuario, y es responsabilidad de cada uno como es el manejo de sus contraseñas, sin embargo se les recomendó tener contraseñas sólidas y no anotarlas en hojas cerca a los equipos, teniendo en

cuenta que cualquier persona puede obtener ese acceso y robar información vital de la compañía, todos los equipos se encuentran inventariados, y en caso de que deban sacar los equipos de las instalaciones, manejan planillas de salida de equipos, en donde se registran las características del equipo, la persona a cargo, el día de salida y el día de ingreso, para tener un control de lo que tienen, en caso de fallas eléctricas cuentan con UPS de respaldo para salvaguardar la información que en esos momentos se esté trabajando, se deben realizar mantenimientos preventivos a los servidores, equipos y UPS para garantizar su buen funcionamiento.

Los niveles de temperatura y humedad relativa en el Centro de Cómputo deben ser mantenidos dentro de los límites requeridos por la infraestructura de cómputo allí instalada, para lo cual se deben usar sistemas de aire acondicionado.

Se debe monitorear y revisar de manera permanente el estado de los componentes de soporte físico, eléctrico y ambiental que hacen parte del Centro de Cómputo, como son el sistema de aire acondicionado, UPS y el sistema de detección y extinción de incendios en caso de existir, entre otros.

En caso de que el canal de comunicaciones contratado llegue a fallar, la empresa cuenta con un proveedor de servicios alterno, con el fin de garantizar la continuidad de las labores.

Cumplimiento de la política de escritorio limpio y pantalla limpia, los puestos de trabajo deben estar limpios de papeles, soportes de almacenamiento extraíbles y cuando un computador este desatendido deberá bloquearse la pantalla.

Cuando sea apropiado, papeles y medios de información deben estar asegurados en armarios especiales, especialmente en horas fuera de las normales de trabajo.

Información confidencial y crítica para T&S COMP. Tecnología y Servicios S.A.S o para el cliente al cual este asignado el contratista debe ser asegurada preferiblemente en armarios resistentes a impacto, fuego e inundación. Los computadores personales no se deben dejar dentro de sesión, se recomienda el uso de llaves físicas, contraseñas, y otro tipo de controles cuando no estén en uso.

Se recomienda la implementación de los objetivos de control de seguridad física y del entorno, en donde se realicen mantenimientos preventivos a todos los equipos cada 6 meses, llevar un control en cuanto a las áreas restringidas de las instalaciones, para que personal no autorizado no ingrese a esas zonas sin los permisos pertinentes. También se debe establecer un monitoreo de los equipos y activos que se encuentren fuera de las instalaciones, garantizando que el personal haga un buen uso de los activos y no perjudique a la empresa.

9.3.8 Seguridad de las operaciones A12. Para los procedimientos operaciones y responsabilidades se tienen definidos algunos procesos de gestión de proyectos, pero no se encuentran documentados y no están actualizados, además no tienen contemplado realizar estudios en cuanto a la capacidad de la infraestructura informática.

Los procedimientos de operación deben ser documentados y puestos a disposición de los usuarios que los necesiten, esta labor está acompañada por el Coordinador IT, quien debe garantizar la documentación y la actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica de T&S COMP. Tecnología y Servicios S.A.S.

El departamento de sistemas debe garantizar que todo cambio realizado a la plataforma tecnológica, quede documentado y se realice su debido seguimiento, certificando y manteniendo sus niveles de seguridad.

Se debe supervisar el uso de los recursos, para realizar los ajustes pertinentes y poder establecer las proyecciones en cuanto a la necesidad de capacidad de infraestructura tecnológica, para garantizar a futuro el rendimiento adecuado del sistema.

Para la protección contra códigos maliciosos no se tiene implementado un control al personal, se le han realizado campañas de concientización pero no han sido efectivas porque no le dan la importancia necesaria, por lo tanto, el Departamento de sistemas debe garantizar que los activos de información, así como los recursos tecnológicos, se encuentren actualizados, evitando códigos maliciosos y virus, que se ejecuten automáticamente, además debe garantizar lo siguiente:

- El software usado para la mitigar los virus informáticos, debe contar con las licencias de uso aprobadas, garantizando su autenticidad y su periódica actualización.
- La información almacenada en los activos de información tecnológicos que es transportada por la red de datos, debe ser escaneada a diario para garantizar así la seguridad de la misma.
- Los usuarios de los activos de información tecnológicos, no pueden modificar la configuración establecida para el software antivirus, esta labor es única y exclusivamente del Coordinador IT.

Los usuarios que manejan los activos de información y recursos informáticos deben garantizar que las descargas de archivos adjuntos de los correos electrónicos o descargas de internet, provienen de fuentes confiables, seguras y exclusivas de acuerdo con las funciones encomendadas.

Los usuarios que manejan los activos de información, deben comunicar al Departamento de Sistemas, cuando encuentren algún virus y no sepan que acciones tomar al respecto para evitar que se ejecute.

Se realizan copias de seguridad en discos duros semanalmente con réplica en tiempo real. Los discos están cifrados y almacenados en el datacenter en donde cuentan con control de acceso biométrico. El encargado de realizar las copias de seguridad es el Coordinador IT. También almacenan el árbol de la información en la nube, y es guardado a diario. Se realiza el seguimiento de todo lo que se almacena a diario en el árbol de la información.

El Departamento de sistemas debe velar por el cumplimiento del procedimiento de copias de respaldo de la información. Los dueños de la información deben almacenar a diario la información en el árbol, previsto por el Coordinador IT. Se deben realizar copias de respaldo de las bases de datos que contienen los sistemas de información empresariales y demás servicios de la empresa a diario. Esta labor debe realizarse de forma automática y monitoreada por el Coordinador IT.
Para el registro y seguimiento, se realiza monitoreo a los empleados por medio de los Logs, para saber en qué momento efectúan los ingresos al sistema. Todas las actividades serán registradas, y esos registros serán protegidos y revisados con periodicidad semanal, por parte de del Coordinador IT.

Se debe implementar la política de sincronización de relojes que deberá ser establecida y documentada.

Control de software operacional: el único que tiene los permisos para poder realizar las instalaciones del software en los sistemas operativos es el Coordinador IT, quien es el encargado de verificar en qué casos se debe realizar la instalación y bajo los parámetros de seguridad y licenciamiento exigidos por la ley.

La empresa T&S COMP. Tecnología y Servicios S.A.S no cuenta con pruebas de vulnerabilidad tanto internas como externas de la infraestructura tecnológica para determinar las posibles vulnerabilidades a las que están expuestos los activos de información y que pueden afectar la Confidencialidad, Integridad y Disponibilidad.

Por parte del Coordinador IT y la alta gerencia no se han realizado auditorías referentes a la Seguridad de la Información. En el momento se encuentran en proceso de implementación, por tanto, se deben realizar auditorías cada 3 meses, con el fin de establecer la verificación de los sistemas de información para garantizar en lo posible interrupciones en los procesos.

Se recomienda establecer la política de Seguridad en las operaciones en donde se determinen y se documenten todos los procedimientos. En cuanto a cambios que se generen en la organización, realizar el seguimiento al uso de los recursos y

determinar la capacidad de la infraestructura tecnológica. Además, se debe realizar las pruebas de vulnerabilidades cada 3 meses, para establecer las falencias y poder mitigar las amenazas presentadas y establecer auditorías para detectar los posibles eventos de seguridad que se estén presentando en la empresa T&S COMP. Tecnología y Servicios S.A.S.

9.3.9 Seguridad de las comunicaciones A13. Para la gestión de la seguridad de redes cuentan con controles como: Cada 90 días el sistema ordena cambiar las contraseñas directamente por el dominio, a cada empleado se le asigna una contraseña y se estipula que es intransferible, con único uso y responsabilidad de cada usuario, cada ingreso al sistema queda grabado en el directorio activo y se recomienda tener claves sólidas con caracteres alfanuméricos. En la página web de la empresa tiene información corporativa, pero la página web no está asegurada por medio de certificados de seguridad, cuentan con un proveedor alterno de servicio de internet, teniendo en cuenta que en una ocasión el servicio fue suspendido por una falla y la empresa no contaba con una contingencia.

La plataforma tecnológica de T&S COMP. Tecnología y Servicios S.A.S., que soporta los sistemas de Información debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones de redes con terceros y del servicio de acceso a Internet. La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad si así se requiere. El Departamento de Sistemas es el área encargada de establecer el perímetro de seguridad necesario para proteger dichos segmentos de acuerdo con el nivel de criticidad del flujo de la información transmitida.

Es responsabilidad de los administradores de recursos tecnológicos garantizar que los puertos físicos y lógicos de diagnóstico y configuración de plataformas que soporten sistemas de información deban estar siempre restringidos y monitoreados con el fin de prevenir accesos no autorizados. Esta labor debe estar acompañada por el Coordinador IT.

No cuentan con la red segmentada, han realizado cotizaciones, pero aún no lo han implementado. Actualmente la transferencia de información se realiza por intermedio del correo corporativo, sin tener protección de la información.

Se debe segmentar la red, para tener una mayor seguridad en las redes donde se hacen las transferencias de información. El Departamento de Sistemas debe proveer los recursos necesarios con los cuales sea posible garantizar el correcto, adecuado y seguro intercambio de información desde estaciones de trabajo y equipos portátiles, así, como desde los dispositivos externos o móviles. Asimismo, debe garantizar que las transacciones de T&S COMP. Tecnología y Servicios S.A.S realizadas de manera electrónica o haciendo uso de las redes de

comunicaciones, cuenten con los controles suficientes para evitar transmisiones incompletas, enrutamiento no apropiado o erróneo, repeticiones de las mismas no autorizadas, pérdida de confidencialidad, integridad de las mismas y pérdida de disponibilidad del servicio.

Por parte de la alta gerencia y teniendo en cuenta las disposiciones legales, en los contratos iniciales a los empleados se les exige el cumplimento del acuerdo de Confidencialidad y no divulgación de la información de la empresa. A terceros también se les exige cumplir con el acuerdo en cada uno de los proyectos de los cuales son participes y tienen personal en sitio.

Se recomienda implementar políticas de seguridad de las comunicaciones de acuerdo a los parámetros dados anteriormente, en donde existan controles para la transferencia de la información, evitando perdidas de ésta. También se debe exigir el cumplimiento de los acuerdos de confidencialidad. Se sugiere bloqueo de acceso de contenidos pornográficos, y descargas no autorizadas, y establecer la segmentación de la red.

9.3.10 Adquisición, desarrollo y mantenimiento de sistemas A14. Los requisitos de seguridad de la información son establecidos por parte de los clientes en donde se desarrollan los proyectos. Por esta razón, teniendo en cuenta que la empresa trabaja por medio de procesos licitatorios con el estado, la información que manejan es de alta confidencialidad.

La información tratada por las aplicaciones aceptadas por la empresa debe preservar su confidencialidad e integridad desde su ingreso, transformación y entrega al negocio. Cada aplicación válida que use y/o transforme información del negocio, debe establecer los medios que preserven su integridad y confidencialidad. Cada solución de información o de infraestructura debe mantener durante su ciclo de vida una gestión de riesgo que informe permanentemente el nivel de exposición que representa para la empresa. Cualquier cambio en el ciclo de vida de un elemento de la plataforma de operación de T&S COMP. Tecnología y Servicios S.A.S debe seguir los procesos de Control de Cambios y Acreditación de la instalación para que preserve el cumplimiento de la Política.

La empresa T&S COMP. Tecnología y Servicios S.A.S no realiza desarrollo de software y componentes de uso interno, no tienen establecidos controles para mitigar los riesgos en el uso de sus aplicativos.

El Departamento de Sistemas debe contar con un grupo de personas el cual debe autorizar la creación, adaptación o adquisición de software. Además, debe estar en constante monitoreo para establecer los mantenimientos preventivos y actualizaciones pertinentes a los sistemas de información; este monitoreo se debe

realizar cada 3 meses, dirigido por el Coordinador IT y con la compañía de la Alta Gerencia.

9.3.11 Relaciones con los proveedores A15. Se acordará con el proveedor y se documentarán los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de T&S COMP. Tecnología y Servicios S.A.S.

De igual forma se debe incluir un acuerdo formal de niveles de servicios en Seguridad de la Información en el que se detallen los compromisos en el cuidado de los recursos de Información de la empresa en la que se va a trabajar y las sanciones en caso de incumplimiento.

Tratamiento del riesgo dentro de acuerdos con proveedores: los requisitos de seguridad de la información pertinentes serán establecidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar, o proporcionar los componentes de infraestructura de TI para la información de T&S COMP. Tecnología y Servicios S.A.S, además, se debe asegurar los activos de la empresa, que son manejados por terceros como proveedores, en donde se debe firmar un acuerdo entre las partes, para el mantener el buen uso de la información confidencial.

Gestión de la prestación de servicios por proveedores, cada servicio con proveedor deberá tener con un supervisor encargado de revisar y auditar la prestación de servicios de proveedores, garantizando el cumplimiento de sus obligaciones contractuales.

El seguimiento y monitoreo de los proveedores debe ser realizado por el Coordinador IT, quien será el responsable de velar por el cumplimiento de las políticas se Seguridad de la Información. El monitoreo se debe realizar cada 6 meses o cuando un nuevo proveedor ingrese a la empresa.

9.3.12 Gestión de incidentes de seguridad de la información A16. La priorización del tratamiento de los incidentes se realiza conforme a la criticidad de la Información. El responsable de la información debe definir los eventos considerados como críticos junto con sus respectivas alertas y registros de seguridad de la información, los cuales deberán ser generados. Éstos deben ser activados, vigilados, almacenados y revisados permanentemente, y las situaciones no esperadas deben ser reportadas de manera inmediata al equipo de respuesta a Incidentes. Los registros y los medios que los generan y administran deben ser protegidos por controles que eviten modificaciones o accesos no autorizados, para preservar la integridad de las evidencias. El encargado de este proceso es el Coordinador IT.

Los empleados deben estar informados del proceso disciplinario que se llevará a cabo en caso de incumplimiento de la Política de Seguridad de la Información o alguno de los elementos que la soportan. En cualquier caso, se hará un seguimiento de acuerdo con los procedimientos establecidos para el manejo de incidentes de seguridad.

Por parte del personal de la empresa T&S COMP. Tecnología y Servicios S.A.S, se debe informar sobre los eventos de seguridad de información. Los eventos de seguridad de información se comunicarán a través de canales de gestión adecuadas tan pronto como sea posible, con el fin de establecer las medidas necesarias para poder mitigarlos lo más pronto posible.

Se debe notificar los puntos débiles de la seguridad de la información, los empleados y contratistas que utilizan los sistemas y servicios de información deben observar y reportar cualquier debilidad de seguridad de información sospechosa en los sistemas o servicios en los que están inmersos. Por parte del Departamento de sistemas se debe llevar un registro de eventos con una periodicidad mensual, para poder llevar un control de ellos y poder mitigarlos para evitar que se materialicen. Además, se deben establecer capacitaciones al personal en donde se indique cual es el procedimiento a seguir cuando se genere un incidente de seguridad, el cual debe ir documentado para evitar que se reporten eventos que no tienen relevancia y enfocarse en los de más alto valor. El reporte oportuno constituye una alerta temprana de riesgos potenciales que puedan afectar a la empresa disminuyendo el impacto de los mismos.

Para la valoración de eventos de seguridad de la información y toma de decisiones, el Departamento de Sistemas, en cabeza del Coordinador IT, es el encargado de valorar los eventos de seguridad de información y decidir si han de ser clasificados como incidentes de seguridad de la información. Todo reporte de incidente de seguridad debe tener una respuesta por parte del Departamento de sistemas de acuerdo a los procedimientos establecidos por la empresa, los cuales deben estar documentados y al alcance de todo el personal.

Cada vez que se presente un incidente de Seguridad de la Información, se debe establecer campañas de concientización en donde sirva de ejemplo para evitar que incidentes del mismo tipo se vuelvan a presentar a futuro y así tener unas mejores prácticas de Seguridad de la Información. Mes a mes debe haber un reporte y en caso de que no exista tal reporte, las áreas de la empresa deben justificar por qué no se reportó ningún incidente para verificar que la gestión se esté haciendo de manera efectiva.

9.3.13 Aspectos de seguridad de la información de la gestión de continuidad de negocio A17. Los procesos críticos establecidos por el T&S COMP.

Tecnología y Servicios S.A.S., deben garantizar que sus activos de información estén disponibles para su tratamiento autorizado cuando se requiera en la ejecución de sus tareas regulares. Se debe definir e implementar un proceso para reducir la interrupción causada por desastres naturales, accidentes y fallos de seguridad por medio de la combinación de controles preventivos y de recuperación.

Es responsabilidad del Departamento de Sistemas, en cabeza del Coordinador IT, diseñar, implementar, probar y mantener su Plan de Continuidad.

El plan de continuidad debe considerar los siguientes aspectos:

- Procedimientos de contingencia los cuales describen las acciones a tomar cuando ocurre un incidente que interrumpe las operaciones del negocio, proporcionando mecanismos alternos y temporales para continuar con el procesamiento.
- Procedimientos de recuperación los cuales describen las acciones a seguir para trasladar las actividades del negocio a un centro alterno de recuperación.
- Procedimientos de retorno los cuales describen las acciones a seguir para regresar las operaciones normales a las instalaciones originales.
- Programación de pruebas las cuales describen la periodicidad en que el plan de continuidad debe ser probado mínimo una vez al año.
- Actualización periódica: El plan debe actualizarse cuando cambios realizados en el ambiente operativo impacten su funcionalidad.
- Consideraciones de seguridad: Es importante que el plan sea diseñado para mantener los controles de seguridad establecidos por la empresa, aun cuando se opere en modalidad de contingencia. Es responsabilidad de la Coordinación de Seguridad de la Información asegurar que estas consideraciones sean efectivamente contempladas en el plan.
- El proceso de copia y respaldo de la información de T&S COMP. Tecnología y Servicios S.A.S, debe contar con una Política que debe cumplir con los requerimientos del negocio, los de seguridad de la información y los legales. Este proceso junto con sus procedimientos es la entrada para la ejecución de los planes de Continuidad de T&S COMP. Tecnología y Servicios S.A.S en caso de presentarse un evento que amerite la activación del Plan.

La empresa T&S COMP. Tecnología y Servicios S.A.S., cuenta con algunos controles para la gestión de continuidad del negocio como se puede observar en el cuadro 20, entre lo que se encuentra lo siguiente:

Cuadro 20. Mantenimiento preventivo por equipo informático T&S COMP. Tecnología y Servicios S.A.S.

Mantenimiento preventivo por equipo informático		
Equipo	**Acción Preventiva/Correctiva**	**Responsable**
Computadores De Escritorio Y Portátiles	Revisión, limpieza interna y externa de todos los componentes. Revisión de virus	Departamento de Sistemas en coordinación con el Departamento de Servicio quien asigna el técnico para la ejecución de la acción.
Impresoras	Revisión, limpieza y lubricación interna y externa de todos los componentes.	Departamento de Sistemas en coordinación con el Departamento de Servicio quien asigna el técnico para la ejecución de la acción.
Servidores	Se realiza un monitoreo a través de acciones manuales en cada servidor. Revisión, limpieza interna y externa de todos los componentes.	Departamento de Sistemas
Fuente: Departamento de sistemas T&S COMP. Tecnología y Servicios S.A.S.		

En la tabla 2 se detalla la relación de los niveles de prioridad con su puntaje que se aplicarán a los Sistemas de Información implementados en T&S COMP. Tecnología y Servicios S.A.S.

Tabla 2. Niveles de prioridad de sistemas de información.

Niveles de prioridad de sistemas de información	
Prioridad	**Puntaje**
Baja	1
Media	2
Alta	3
Fuente: Autores.	

A continuación, en el cuadro 21 se muestra la lista de sistemas de Información orientados por prioridad de restauración (desde la máxima prioridad hasta la más baja), que son necesarios para garantizar una continuidad de la operatividad y servicios que ofrece T&S COMP. Tecnología y Servicios S.A.S ante un desastre o siniestro:

Cuadro 21. Niveles de prioridad de sistemas de información T&S COMP. Tecnología y Servicios S.A.S.

Sistemas de información / servicios implementados					
Sistema de información	**Proveedor**	**Plataforma**	**Lenguaje de programación**	**Usuarios**	**Prioridad**
HELISA	Externo (HELISA)	Windows Firebird		Facturación y recaudo Mayorista EPSON Almacén Compras	3
VTIGER	Externo (VTIGER)	Bajo Windows MYSQL	PHP, JAVASCRIPT	TODOS LOS PROCESOS	2
ARANDA	Externo (ARANDA)	Bajo Windows SQL	PHP, JAVA SCRIP ASP.NET	TODOS LOS PROCESOS	1
OCS INVENTORU	Externo (GNU GPLv2)	Bajo Windows, Linux SQL	PHP SQL JAVA SCRIP	SISTEMAS	1
Fuente: Departamento de sistema T&S COMP. Tecnología y Servicios S.A.S.					

La referida gestión tiene como finalidad identificar los riesgos, establecer los procedimientos y mecanismos para preservar la seguridad de los equipos de cómputo y servidores, proteger la información almacenada en ellos, y garantizar la continuidad de las funciones de la empresa T&S COMP. Tecnología y Servicios S.A.S.

9.3.14 Cumplimiento A18. Deben establecerse procedimientos apropiados para asegurar el cumplimiento con las restricciones de carácter legal en el uso de material que puede estar sujeto a derechos de propiedad intelectual tales como derechos de autor y derechos de diseño.

Identificación de la legislación aplicable y los requisitos contractuales: todos los requisitos pertinentes, legislativos estatutarios, reglamentarios y contractuales, y el planteamiento de la entidad para cumplir con estos requisitos deberán estar

explícitamente identificados, documentados y protegidos al día para cada sistema de información y la organización.

Los registros deben estar protegidos contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de conformidad con los requisitos de legalidad, reglamentarias, contractuales y comerciales.

Se debe garantizar la privacidad y la protección de la información de identificación personal a lo dispuesto en la legislación y la reglamentación pertinente.

Regulación de los controles criptográficos: los controles criptográficos serán utilizados en cumplimiento a todos los acuerdos pertinentes, la legislación y los reglamentos.

El enfoque de la organización para la gestión de seguridad de la información y su aplicación, es decir, los objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información, se revisará de forma independiente a intervalos planificados o cuando se produzcan cambios significativos.

El Departamento de Sistemas deberá comprobar periódicamente el cumplimiento de los procedimientos de procesamiento de la información dentro de su área de responsabilidad con las políticas de seguridad, las normas y otros requisitos de seguridad, se debe auditar mínimo una vez al año para verificar la aplicación, completitud y cumplimiento de las políticas de Seguridad de la Información.

Periódicamente se debe evaluar el cumplimiento de los requerimientos de seguridad por parte de los usuarios. El incumplimiento de los requerimientos de seguridad, se debe registrar como un incidente a la Política de Seguridad de la información que debe ser resuelto de acuerdo con los procedimientos de manejo de incidentes de T&S COMP. Tecnología y Servicios S.A.S.

Las situaciones o acciones que violen la presente Política deben ser detectadas, registradas, analizadas, resueltas e informadas al comité de Seguridad de la Información y a las áreas responsables por su tratamiento de manera inmediata.

11. RESULTADOS

¿Cómo se puede establecer la integridad, disponibilidad y confidencialidad de la información en un modelo de negocio orientado a la prestación de servicios tecnológicos?

Para establecer la integridad, disponibilidad y confidencialidad de la información en un modelo de negocio orientado a la prestación de servicios tecnológicos, se deben adoptar procesos adecuados para la planeación, implementación, mantenimiento y mejora del SGSI, de acuerdo a la norma ISO 27001:2013

Por medio del diseño del Sistema de Gestión de Seguridad de la Información, conociendo como es el manejo de la información en cada uno de los procesos de la empresa T&S COMP. Tecnología y Servicios S.A.S, se determinaron cuáles son las vulnerabilidades y posibles amenazas, identificando los diferentes riesgos que afectan a la empresa para evitar que se materialicen. Por esto, por medio de mejores prácticas fomentadas desde la alta gerencia, se crea un ambiente de cultura de Seguridad de la Información a todas las partes interesadas en el desarrollo de la prestación de su servicio.

Teniendo en cuenta que el modelo de negocio está orientado a la prestación de servicios tecnológicos, en donde la información es un activo vital, que puede ser alterado, divulgado y no disponible, es necesario aplicar los diferentes planes de tratamiento apoyados en los controles de la norma ISO 27001:2013. Para tener un adecuado uso y manejo de la información vital de la empresa, se debe tener en cuenta que estos servicios son ofrecidos en su mayoría a empresas del estado y es de vital importancia poder brindar seguridad y confianza a los clientes, garantizando el buen uso de la información brindada por las partes.

12. CONCLUSIONES

- Las Pequeñas y medianas empresas, como T&S COMP. Tecnología y Servicios S.A.S, con la innovación tecnológica, se enfrentan a riesgos que pueden generar daños irreparables en el desarrollo de las actividades de las organizaciones. Con el diseño del Sistema de Gestión de Seguridad de la Información en la empresa, ayudó a establecer mecanismos para la protección de los activos de información y tomar precauciones para asegurar los sistemas que procesan esa información.

- Para el diseño de Sistema de Gestión de Seguridad de la Información en T&S COMP. Tecnología y Servicios S.A.S, se contó con la participación de la alta dirección y el respaldo de todos los procesos, teniendo en cuenta que son los principales interesados en que se incluyan estándares de Seguridad Informática necesarios. Con esto, tanto sus funcionarios, clientes y proveedores tienen la certeza que se utilizan buenas prácticas para la protección de su información logrando aumentar su confianza en la empresa.

- La Seguridad de la Información es fundamental en los diferentes procesos que se manejan en la empresa, sin embargo, el personal no toma el tema de la seguridad de la información como importante y no da prioridad a los activos de información que son vitales para la empresa. Con el diseño del Sistema de Gestión de Seguridad de la Información, ayudó a establecer procedimientos y buenas prácticas para manejo óptimo para el desarrollo de las actividades de la empresa y a cumplir con los requisitos legales teniendo en cuenta la Confidencialidad, Integridad y Disponibilidad de su información.

- El análisis de riesgos contribuyó a detectar las amenazas a las que la organización está expuesta, frente a la inadecuada gestión de conocimiento de sus activos de información, lo que les permitió reconocer los riesgos a los que se enfrentan y el impacto que puede originar si se materializan. Para los riesgos que resultaron inaceptables, se enfocaron esfuerzos para realizar una acción inmediata con el fin de generar controles para mitigarlos y crear valor a los activos de información de cada uno de los procesos.

- La gestión efectiva de la Seguridad de la Información debe estar inmersa desde la alta gerencia, empleados, clientes y proveedores, en donde cada uno tiene un rol importante para que el cumplimiento de controles y políticas sea todo un éxito. Asimismo, se garantiza el buen uso de la información, mitigando en lo posible todos los riesgos que se generan en los diferentes procesos y saber cómo actuar, para tener una buena toma de decisiones,

llegar asumir los riesgos residuales que sean mínimos, y mantener un buen estado de seguridad de la información, con un monitoreo constante.

BIBLIOGRAFÍA

ALCALDÍA MAYOR DE BOGOTÁ. Ley 527 de 1999 [Online]. [Consultado 31 de enero de 2016]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276

ALCALDÍA MAYOR DE BOGOTÁ. Ley Estatutaria 1581 de 2012 [Online]. [Consultado 20 de diciembre de 2016]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

ALCALDÍA MAYOR DE BOGOTÁ. Ley Estatutaria 1581 DE 2012 [Online]. [Consultado 20 de diciembre de 2016]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

ALTA CONSEJERÍA DISTRITAL DE TIC. Autodiagnóstico SGSI V2 [Online]. [Consultado 16 de enero de 2017]. Disponible en: tic.bogota.gov.co/sites/default/files/.../AutodiagnosticoSGSI_v2_09072015.xls

DEPARTAMENTO NACIONAL DE PLANEACIÓN, Guía metodológica para la administración de riesgos del SGSI [online]. [Consultado 15 de febrero de 2017]. Disponible en: https://colaboracion.dnp.gov.co/CDT/DNP/SE-G02%20Gu%C3%ADa%20metodol%C3%B3gica%20para%20la%20admon%20de%20riesgos%20del%20SGSI.Pu.pdf?

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, ISO 27000. [Online]. [Consultado 25 de abril de 2016]. Disponible en: http://www.iso27000.es/download/doc_iso27000_all.pdf

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, ISO 27000. [Online]. [Consultado 25 de febrero de 2017]. Disponible en: http://www.iso27000.es/glosario.html

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO 31000:2009 - Risk management. Principles.

MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Guía para la Gestión y Clasificación de Activos de Información. Clasificación de activos de la información.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Glossary of Key Information Security Terms. [Online]. [Consultado 17 de diciembre de 2016]. Disponible en: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf.

PORTAFOLIO, 'La seguridad informática se contrajo 15 % en ventas'. [Online] [Consultado el 25 de abril de 2016]. http://www.portafolio.co/negocios/la-seguridad-informatica-se-contrajo-15-ventas

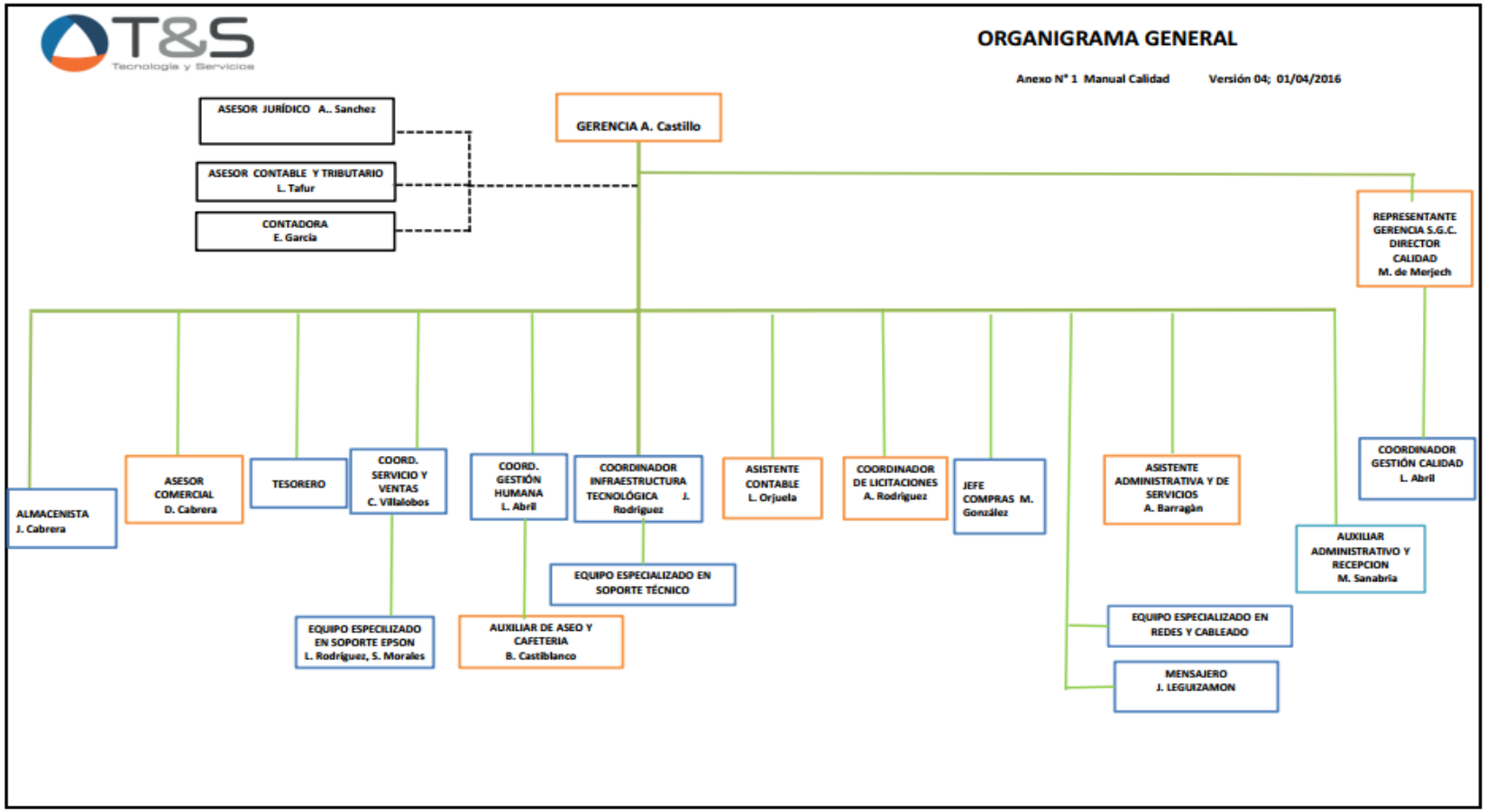
T&S COMP. TECNOLOGÍA Y SERVICIOS S.A.S. Generalidades de la empresa. [Online] [Consultado el 25 de abril de 2016]. http://tyscomp.com/nosotros/

TCPSI. Dominios de la norma ISO 27001:2013 [Online]. [Consultado 21 de enero de 2017]. Disponible en: http://www.tcpsi.com/vermas/iso_27001.htm

ANEXOS

Anexo A. Organigrama empresa T&S COMP. Tecnología y Servicios S.A.S

Figura 7. Organigrama T&S COMP. Tecnología y Servicios S.A.S



Anexo B. Encuesta Interesados Internos y Externos

ANÁLISIS DE INTERESADOS:

INTERNOS Y EXTERNOS: líderes de procesos, directicas, clientes, mercadeo

1. **¿Qué tipo de interesados internos tienen?**

Respuesta: Líderes de procesos, directivas

2. **¿Qué tipo de interesados externos tienen?**

Respuesta: Clientes y proveedores

3. **¿Qué expectativa y necesidades tiene respecto a la Seguridad de la Información en la labor que realiza?**

Respuestas:

Gerencia: Poder salvaguardar la información vital de la empresa, por medio de buenas prácticas de seguridad de la información.
Coordinador IT: Mantener un control constante sobre la seguridad de la información de T&S, es necesario establecer los procedimientos para dichos controles.
Coordinadora de Licitaciones: Teniendo en cuenta la naturaleza de la información, debe existir una seguridad que garantice que los archivos no serán alterados, así mismo es importante que los accesos los tengan solo las personas que intervienen en el proceso.
Jefe de compras: La seguridad de los proveedores, y la de backordes.
Tesorero - control interno: Confidencialidad en la información manejada.
Empleado: resguardar la información de clientes en temas de cobros a servicios realizados.
Proveedores: Prolongación en la contratación, cumplimiento en pagos y protección de la información personal.
Clientes: Protección de la operación para que le aseguren servicio seguro, así como su información personal.

4. **¿Qué forma considera que sería la mejor para satisfacer esa necesidad?**

Respuestas:

Gerencia: Poder salvaguardar la información vital de la empresa, mediante un Sistema de Gestión de Seguridad de la Información.
Coordinador IT: concientización a los líderes de procesos sobre la importancia y peligros que se deben tener en cuenta en el manejo de la información del día a día.
Coordinadora de Licitaciones: Los accesos que intervienen en el proceso.
Jefe de compras: Bloqueo de la información a las personas que no corresponden.
Tesorero - control interno: Restringiendo acceso a personal no autorizado.
Empleado: es una buena alternativa, pero tendría que tener un tema de perfiles de usuarios editores para mayor resguardo y de igual forma el realizado de backup del mismo por si en algún momento se cae el sistema.
Proveedores: Establecer controles con cada uno de los contratos que se establezcan con los proveedores, garantizando la confidencialidad de la información suministrada.
Clientes: Estricto cumplimiento de las leyes de protección y manejo de los datos personales, garantizando la confidencialidad de la información suministrada.

ROLES Y RESPONSABILIDADES

1. **¿Existe un oficial de la seguridad en la empresa, si no existe quien podría desarrollar el rol y cuáles serían sus responsabilidades?**

Respuesta:
No contamos con un oficial de seguridad y la persona encargada es el coordinador de sistemas.

2. **¿Cuál es el rol del grupo de calidad, que responsabilidades tienen?**

Respuesta:
Verificar la eficacia tanto de clientes, correctivos que se deban hacer, las políticas y objetivos de calidad, bajo la norma de calidad ISO 9001:2008.

PROCESO ESTRATÉGICO:

1. **¿Qué activos vitales tienen o se manejan en este proceso?**

Respuesta:
Los manuales de calidad, las políticas de calidad, los objetivos de calidad, el plan estratégico, listado maestro de registros, red de procesos, procedimientos de control, toda esta esta información va documentada y debe ir en el árbol de la información.

2. **¿Cuáles son los roles y responsabilidades de los encargados del proceso?**

Respuesta:

- Tiene la responsabilidad de verificar y aprobar el Sistema de Gestión de Seguridad de la Información (SGSI).
- Realizar seguimiento al cumplimiento de las políticas
- Establecer un monitoreo anual, en donde se realice auditoría a todo el sistema
- Revisar mensualmente el sistema de gestión de calidad
- Revisar la eficacia de cada proceso
- Tomar acciones preventivas y de mejora

Proceso Gerencial

Proceso Sistema Gestión Calidad (S.G.C.)

1. **¿Bajo qué norma de calidad se rige la compañía?**

Respuesta:
ISO 9001:2008

2. **¿En qué consisten las auditorías internas?**

Respuesta:
Se realizan planes de auditoría, en especial por cada proceso, hace revisión del sistema de gestión de calidad.

3. **¿Cada cuánto revisan el sistema de gestión de calidad?**

Respuesta:
La revisión se hace mensualmente por parte del líder de calidad.

4. **¿En qué consisten las acciones preventivas, correctivas y mejora?**

Respuesta:
Consisten en revisar la eficacia y el cumplimiento de las políticas y objetivos de calidad, además trata de las no conformidades y que hacer para que vuelvan a suceder.

PROCESOS MISIONALES:

- Proceso Servicios (Administración y logística – CSA Epson)
- Proceso Comercial (Comercial Mayorista Epson – Licitaciones)

1. **¿Qué activos vitales tienen o se manejan en este proceso?**

Respuesta:
Informes mensuales, indicadores de servicio, base de datos de los clientes, consolidado de facturación de los clientes, cotización aprobadas y generales, ofertas técnicas y económicas, información de los clientes.

2. **¿Cuáles son los roles y responsabilidades de los encargados del proceso?**

Respuesta:
- Establecer estrategias de mercadeo, para participar en procesos licitatorios.
- Elaborar y presentar propuestas a los posibles clientes
- Facturar y recaudar lo correspondiente a los servicios prestados
- Analizar los indicadores de gestión
- Tomar acciones preventivas y de mejora
- Procesos propios de la Estructura del negocio y que guardan relación directa con los clientes.

3. **¿Cómo almacenan las bases de datos y cuantas personas tienen acceso a esa información?**

Respuesta:
Las bases de datos son almacenadas en el directorio activo, que a su vez es almacenado en el árbol de la información.
Dos personas son las encargadas de manejar la base de datos, el de administración y servicios, y procesos licitatorios.

4. **¿Cómo se puede ver afectado un producto del portafolio de servicios, por un riesgo de seguridad informática?**

Respuesta:
Se puede ver afectado principalmente por la competencia, en donde se puede ofrecer el mismo servicio, pero con mejores garantías, puede haber suplantaciones de identidad, por parte de un tercero ofrecer los mismos productos sin ser empleado de la empresa, generando así ganancias y perjudicando la imagen de la empresa.

PROCESOS DE APOYO:

1. **¿Qué activos vitales tienen o se manejan en este proceso?**

Respuesta:
Firewall herramienta Smoothwall, servicios de dominio, soporte Aranda Service Desk, aplicativo Helisa, CloudBerry, Network inventary, Vtiger CMR, Proxy ClearOS, directorio activo, nómina de empresa.

2. **¿Cuáles son los roles y responsabilidades de los encargados del proceso?**

Respuesta:
<u>Proceso de facturación y recaudo, tesorería:</u>

- Análisis de cartera
- Gestión de cobro de cartera
- Tomar acciones preventivas y correctivas y de mejora.

<u>Proceso de compras y almacén:</u>

- Selección y evaluación de proveedores
- Ejecutar compras de manera confiable
- Evaluar el desempeño y confiabilidad de los proveedores
- Analizar indicadores de gestión
- Tomar acciones preventivas y correctivas y de mejora.

Proceso de gestión humana:

- Reclutamiento, selección y contratación de personal
- Definir el perfil de cada cargo
- Realizar evaluación de desempeño
- Tomar acciones preventivas y correctivas y de mejora.

Proceso de sistemas:

- Apoyo en software y hardware
- Velar por el funcionamiento de los servidores físicos y virtuales
- Controlar y asegurar la información de la empresa
- Tomar acciones preventivas y correctivas y de mejora.

Proceso Compras y Almacén

¿Qué tipo de información manejan los proveedores?
Respuesta:
Referente a los equipos, repuestos e insumos en este caso de Epson.

Proceso Gestión Humana:

¿Qué actividades se manejan en este proceso?
Respuesta:
Lo primero que se realiza es la verificación de antecedentes del personal que va ingresar a la empresa, por medio de la procuraduría y de la policía, se están realizando visitas domiciliarias según sea el caso, en los contratos se establece la cláusula de confidencialidad de la información antes durante y después del empleo, la cual se debe cumplir o tendrán sanciones penales.
Para la contratación de personal en sitio, por temas licitatorios, lo primero que realizan es verificar una base de datos de personal que con anterioridad ya había sido contratado, para tener la certeza de que personal envían a las entidades, para brindar confianza.

Proceso Facturación y Recaudo:

¿Qué actividades se manejan en este proceso?
Respuesta:
Todo el proceso contable es manejado por intermedio del aplicativo Helisa, en el área son dos personas, quienes son el contador y el auxiliar contable.
Proceso Sistemas:

¿Qué actividades se manejan en este proceso?
Respuesta:
Manejamos todo lo referente a los controles de acceso, para cada uno de los usuarios, se establecen roles en el directorio activo para el ingreso, se crean bloqueos de puertos y de páginas no permitidas en la red.

Para controlar y asegurar la información de la empresa, por parte del coordinador IT, se tiene un disco duro el cual está cifrado y se realiza el almacenamiento de la información semanalmente y con una réplica en tiempo real del histórico de la semana.

La información es almacenada en la nube y en discos externos, garantizando la continuidad del negocio en caso de algún incidente catastrófico.

DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN LA EMPRESA T&S. COMP. TECNOLOGÍA Y SERVICIOS S.A.S., EN LOS PROCESOS DE APOYO, MISIONALES Y ESTRATÉGICOS, BASADO EN LA NORMA ICONTEC ISO 27001:2013

Mayra Alejandra Vargas García, Andrés Felipe Zubieta Daza
Especialización en Seguridad Informática, Universidad Piloto de Colombia
mayralejandravg@gmail.com
andres.zubietadaza@gmail.com

***Resumen*— Los activos de información son vitales para el desarrollo efectivo de las organizaciones y en muchas ocasiones no saben cómo salvaguardarlos de una forma adecuada. Por esta razón, T&S COMP. Tecnología y Servicios S.A.S se ve en la necesidad de diseñar un Sistema de Gestión de Seguridad de la Información en los procesos de Apoyo, Misionales y Estratégicos basado en los pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad con el propósito de mantener niveles óptimos de competitividad, rentabilidad e imagen empresarial alineados con los objetivos de la organización.**

***Palabras Clave*— Seguridad de la Información, SGSI, Activo, Confidencialidad, Integridad, Disponibilidad, Análisis de Riesgo, Amenazas, Tratamiento de Riesgo, Mitigar, Políticas, Controles.**

***Abstract*— Information assets are vital to the effective development of organizations and often do not know how to safeguard them in an appropriate way. For this reason, T & S COMP. Technology and Services SAS is in need of designing an Information Security Management System in the Support, Mission and Strategic processes based on the pillars of information security: confidentiality, integrity and availability in order to maintain Optimal levels of competitiveness, profitability and corporate image aligned with the objectives of the organization.**

***Keywords*— Information Security, ISMS, Asset, Confidentiality, Integrity, Availability, Risk Analysis, Threats, Risk Management, Mitigation, Policies, Controls.**

I. INTRODUCCIÓN

UN tema de gran importancia en una organización es la seguridad informática, ésta debe ir alineada con los avances tecnológicos debido al crecimiento de los delitos informáticos que se van presentando a medida del tiempo, y el cual ha provocado daños irreparables y ha generado grandes pérdidas para las empresas víctimas de ataques cibernéticos. Como consecuencia de esto, se ha hecho necesario salvaguardar y proteger la información de la apropiación ilegal de personas que pretenden sacar provecho de vulnerabilidades del gran sistema de información que manejan.

Por tal motivo, este artículo se desarrollará en la empresa T&S COMP. Tecnología y Servicios S.A.S, en la cual se pretende realizar un diseño del Sistema de Gestión de Seguridad de la Información (SGSI), basado en la norma ISO 27001:2013, en los Procesos de Apoyo, los cuales están compuestos por: Compras y Almacén, Facturación y Recaudo, Gestión Humana y Sistemas, los procesos Misionales compuestos por: Comercial y Servicios y los procesos Estratégicos compuestos por Gestión Gerencial y Gestión de Calidad.

T&S COMP. Tecnología y Servicios S.A.S. es una empresa colombiana prestadora de servicios de tecnología con más de 10 años de experiencia en reparación, mantenimiento preventivo y correctivo, y soporte de equipos EPSON en empresas del Estado. Debido a los grandes clientes que la empresa les brinda servicios, se hace necesario implementar un SGSI para la protección de los datos el cual se tiene como reto incrementar la capacidad para descubrir y mitigar amenazas, recuperarse de ataques y actualizar su infraestructura obsoleta que pone en riesgo la información.

II. JUSTIFICACIÓN

Gracias a las grandes transformaciones y ventajas que la tecnología ofrece, también trae consigo cambios que afectan los Sistemas de Información como los ataques informáticos. Este es un tema que para muchas empresas son irrelevantes y no han comprendido lo valiosa que es su información. Uno de los errores más notables que en las empresas se cometen, es pensar que su información no es de interés de nadie y, por lo tanto, no fortalecen sus sistemas de seguridad para salvaguardar la información; lo cual da como resultado una infraestructura tecnológica vulnerada y puede ser el blanco de muchos ciberdelincuentes para obtener información sensible.

Según Jon Parkes, Vicepresidente mundial de Preventa de Intel Security, “En el 2020 habrá en el mundo entre 15 y 16 billones de dispositivos y tienen que comunicarse. Nuestro

negocio es ver cómo esto se hace de una manera segura"[1]. Si bien es cierto, el gran progreso que en un futuro presentarán las Tecnologías de la Información y las Comunicaciones, requiere de un gran esfuerzo por concientizar a las PYME de la importancia y los desafíos que se enfrentan en temas de seguridad por las nuevas tecnologías y las nuevas vulnerabilidades de las que son el principal blanco de los atacantes cibernéticos. Por tal motivo, es sumamente importante generar un acercamiento con las empresas para concientizarlas del valor de resguardar la información sensible que se encuentra almacenada y, que en efecto, es transmitida por elementos y sistemas de información que día a día están expuestos a vulnerabilidades que se presentan con nuevos ataques informáticos.

Como consecuencia de esto, el propósito del proyecto es realizar una concientización, diseño y posterior implementación de un Sistema de Gestión de Seguridad Informática en la empresa T&S COMP. Tecnología y Servicios S.A.S. "T&S es una empresa integradora de servicios y tecnología con más de 10 años de experiencia en el mercado colombiano"[2], a pesar que maneja servicios de tecnología no tiene diseñado un SGSI.

III. OBJETIVOS

A. *Objetivo General*

Diseñar un Sistema de Gestión de Seguridad de la Información en la empresa T&S COMP. Tecnología y Servicios S.A.S, para asegurar la Confidencialidad, Integridad, Disponibilidad y control de la información sensible administrada en los procesos de Apoyo, Misionales y Estratégicos, basados en la norma ICONTEC ISO 27001:2013.

B. *Objetivos Específicos*

- Determinar el contexto actual de la empresa T&S COMP. Tecnología y Servicios S.A.S., y las expectativas en relación con el Sistema de Gestión de la Seguridad de la Información.
- Gestionar y clasificar los activos de información de T&S COMP. Tecnología y Servicios S.A.S de los procesos de Apoyo, Misionales y Estratégicos. en materia de Seguridad de la Información.
- Identificar, analizar y valorar los riesgos de Seguridad de la Información asociados a los procesos de Apoyo, Misionales y Estratégicos de la empresa T&S COMP. Tecnología y Servicios S.A.S, basado en la norma ISO 31000:2009.
- Establecer planes de tratamiento de riesgos de Seguridad de la Información para los procesos de Apoyo, Misionales y Estratégicos de la empresa T&S COMP. Tecnología y Servicios S.A.S.
- Definir políticas de Seguridad de la Información para los procesos de Apoyo, Misionales y Estratégicos de la empresa T&S COMP. Tecnología y Servicios S.A.S.

IV. CONTEXTO DE LA ORGANIZACIÓN

Con el continuo cambio que van presentado de las tecnologías de la información y las comunicaciones, se requiere una dinámica contante para salvaguardar la información por el gran valor que constituyen en las organizaciones. Sin embargo, las PYME están más expuestas a ciberataques ya sea por su inexperiencia o por falta de estructuras de seguridad en su red.

Esta etapa, tiene como objetivo el análisis y conocimiento de la organización para reconocer y determinar que amenazas los afectan tanto interna como externamente, identificar los recursos a proteger y establecer el nivel de riesgo al cual están expuestos los procesos de Apoyo, Misionales y Estratégicos.

T&S COMP. Tecnología y Servicios S.A.S. es una empresa colombiana encargada de prestar servicios tecnológicos como Centro de Servicio Autorizado EPSON (CSA) para brindar reparación y soporte de equipos. Son mayoristas de partes EPSON y ofrecen soluciones en gestión de infraestructura informática junto con Aranda Software. En su interés por asegurar su información, T&S COMP. Tecnología y Servicios S.A.S, orienta sus esfuerzos para la consecución y desarrollo de este proyecto, para ser implementado dentro de su entorno de seguridad.

Para el diseño del SGSI en los procesos de la empresa, basado en la norma ISO 27001:2013, se establecen dos tipos de factores para el análisis de amenazas: internos y externos. Para determinar los factores internos, inicialmente se hace un reconocimiento de la organización como: su objetivo principal, estructura organizacional, procesos y subprocesos, expectativas y precepciones de los involucrados internos, identificación de activos y sistemas de información. Por otro lado, se identifican los externos como: Partes involucradas externas (clientes, proveedores), factores medioambientales y tecnológicos, el ambiente económico, político y social.

A partir de estos factores se identifican las amenazas que intervienen, afectando la seguridad de su información que da como resultado una infraestructura tecnológica vulnerada. Un error que generalmente ocurre en la entidad es la inadecuada gestión de conocimiento sobre el valor que tiene la información y por tanto no fortalecen su sistema de seguridad para salvaguardar la información.

[1] PORTAFOLIO, 'La seguridad informática se contrajo 15 % en ventas'. [Online] [Consultado el 25 de abril de 2016]. http://www.portafolio.co/negocios/la-seguridad-informatica-se-contrajo-15-ventas

[2] T&S COMP. TECNOLOGÍA Y SERVICIOS S.A.S. Generalidades de la empresa. [Online] [Consultado el 25 de abril de 2016]. http://tyscomp.com/nosotros/

A. Matriz DOFA

La matriz DOFA permite enfrentar la diversidad de factores internos (fortalezas y debilidades) y externos (oportunidades y amenazas) en los procesos de Apoyo, Misionales y Estratégicos de la empresa T&S COMP. Tecnología y Servicios S.A.S, generando alternativas y estrategias para mejorar la gestión de TIC enfocadas en la seguridad informática.

Una vez realizado el análisis de la situación actual de la empresa T&S COMP. Tecnología y Servicios S.A.S, se obtuvieron las siguientes estrategias en base a los objetivos de Sistema de Gestión de Seguridad de la Información:

- Establecer un Gobierno de seguridad de la información y los respectivos lineamientos de seguridad para proteger los recursos de la compañía.
- Realizar actualización del inventario de activos de información cada año con el apoyo de todas las áreas.
- Aplicar medidas necesarias para la actualización y clasificación de los activos de información.
- Realizar campañas de concientización al personal de T&S COMP. Tecnología y Servicios S.A.S sobre la importancia de la seguridad de la información en el desarrollo de cada labor.
- Determinar y divulgar las políticas de seguridad informática de acuerdo a las mejores prácticas y lineamientos establecidos en la compañía.
- Definir procesos para el adecuado manejo de la información personal, basados en las buenas prácticas.
- Implementar controles para el manejo de la información personal basado en la ley de protección de datos personales.
- Realizar el escaneo de vulnerabilidades de red mensualmente para identificar las amenazas a las que está expuesta la organización.
- Implementar controles para el escaneo de vulnerabilidades.

B. Análisis de Brecha

Una vez analizada la situación actual de la empresa referente a la Seguridad de la información, identificando cuáles son sus debilidades y fortalezas se determinó el análisis de brecha de acuerdo a los controles del anexo A de la norma ISO 27001:2013.

Teniendo en cuenta la información anterior, se determinó que existen falencias principalmente en los controles de: Políticas de Seguridad de la Información, Gestión de Activos, Control de Acceso y Cumplimiento.

C. Comprensión de necesidades

Los interesados plasmaron sus expectativas y necesidades respecto a la seguridad de la información en la empresa T&S COMP. Tecnología y Servicios S.A.S. Se determinó que varios de los interesados tienen puntos en común para poder satisfacer esas necesidades como las buenas prácticas para el manejo de la información de la empresa y establecer procedimientos para salvaguardar la información tanto a nivel interno como externo. Hicieron énfasis en establecer controles para clientes y proveedores con el fin de evitar pérdida de información, garantizar su integridad y brindar confidencialidad tanto para la empresa como para los clientes y proveedores.

De la misma manera, por medio de políticas de la seguridad de la información se pueden establecer requisitos, para mantener y mejorar el SGSI, con el objetivo de satisfacer sus expectativas como parte integral de la empresa.

V. GESTIÓN Y CLASIFICACIÓN DE ACTIVOS

Los activos son el corazón y la parte fundamental para el pleno desarrollo de las actividades de las empresas, por esto, con una administración efectiva de cada uno de sus recursos se logra un conocimiento de lo que se tiene y una distribución eficaz, adecuada y organizada en el momento que se requiera. El objetivo de los inventarios de activos, es identificar y controlar de forma precisa los recursos existentes en la organización. Por esta razón, se determinará la gestión y clasificación de los activos en los procesos de Apoyo, Misionales y Estratégicos de T&S COMP. Tecnología y Servicios S.A.S.

Esta etapa del SGSI, se identifica y evalúa la importancia de los activos críticos de T&S COMP. Tecnología y Servicios S.A.S., en el que se valoraran en una escala para definir su relevancia en las actividades de la empresa y cumplir con los objetivos del negocio. Una vez identificado el valor de los recursos, se dará paso al análisis de riesgo.

A. Identificación de activos

Las actividades para la clasificación de activos son: identificación, revisión, actualización y publicación; en términos del diseño del sistema, se realiza la identificación de los activos con ayuda de los líderes de los procesos de Apoyo, Misionales y Estratégicos. Se determinaron los siguientes activos:

- Información
- Recurso Humano
- Software
- Hardware
- Instalaciones

B. Valoración de activos:

Para alcanzar el objetivo de valorar los activos críticos de la empresa, se debe tener en cuenta que cuanta mayor criticidad

tenga el recurso, mayor será el riesgo al que está expuesto, por esta razón, en el momento que se presente un evento, la amenaza se puede materializar y puede causar grandes impactos para la organización.

La valoración de los activos de información se determina de acuerdo a los principios de seguridad de la información y a los niveles de protección adecuados basados en su valor:

- Confidencialidad: Se definieron los siguientes niveles: Información pública reservada, Información pública clasificada, información pública y no clasificada.
- Integridad: Se definieron los siguientes niveles: Alta, media, baja y no clasificada.
- Disponibilidad: Se definieron los siguientes niveles: Alta, media, baja y no clasificada.

Para la tabla se registraron los siguientes campos:

- Identificador: Número de identificación del activo.
- Nombre del Activo: Nombre del activo de información de acuerdo al proceso al que pertenece.
- Principio: Protección de la información de acuerdo a la Confidencialidad, Integridad y Disponibilidad del activo de información.
- Clasificación: Valoración de los activos de acuerdo a la criticidad de pérdida del principio de seguridad de la información.
- Justificación: Impacto que causaría la pérdida de Confidencialidad, Integridad o Disponibilidad del activo.

VI. GESTIÓN Y ANÁLISIS DE RIESGOS DE LA SEGURIDAD

Como parte del SGSI en T&S COMP. Tecnología y Servicios S.A.S., se deben considerar los riesgos a los que está expuesta la empresa y determinar oportunidades con el fin que se logren los resultados deseados, prevenir eventos indeseados y obtener una mejora continua mediante la evaluación e implementación de acciones previstas en el tratamiento de los riesgos.

Para la administración adecuada de los riesgos en los procesos de Apoyo, Misionales y Estratégicos de T&S COMP. Tecnología y Servicios S.A.S, como primera medida, se obtuvo el compromiso de la alta dirección, el cual brindó el respaldo para la identificación, evaluación y tratamiento de riesgos, determinó controles y asignó recursos necesarios para su gestión. Por otro lado, se conformó un grupo interdisciplinario encargado de liderar el proceso del SGSI y el posterior análisis de los riesgos, con gran conocimiento en los procesos de la entidad y el canal directo de comunicación con la alta dirección y las otras dependencias.

A. Análisis de riesgos

Para efectos de análisis de riesgo en los procesos de Apoyo, Misionales y Estratégicos de T&S COMP. Tecnología y Servicios S.A.S, se utilizaron las metodologías ISO 31000 e ISO 27005, las cuales proveen las directrices para desarrollar adecuadamente la gestión de riesgos. Se estableció conforme a los objetivos de la empresa y de acuerdo sus necesidades para el mejoramiento del gobierno de Seguridad de la Información. Se determinaron los siguientes puntos para el análisis de riesgos en la empresa:

- Identificación de riesgos: En esta etapa, la identificación del riesgo se realiza con base en los elementos establecidos en el Contexto y el estado actual de la empresa T&S COMP. Tecnología y Servicios S.A.S, la identificación y valoración de activos analizados previamente en el apartado anterior, para determinar los factores que pueden interrumpir el cumplimiento de los objetivos del negocio. Éstas pueden ser internas o externas.
- Identificación de amenazas: Las amenazas son acciones que aprovechan una vulnerabilidad y pueden causar daños potenciales a los activos de información de la empresa.
- Identificación de vulnerabilidades: Las vulnerabilidades son debilidades de los activos de información que pueden ser aprovechados por un ciberdelincuente.

B. Evaluación del riesgo:

Al gestionar el riesgo, se debe valorar y determinar elementos para intervenir incidentes que puedan afectar la organización. El proceso de valoración de riesgos ayuda a estimar la magnitud de las amenazas que están presentes en la empresa y que a través de los planes de tratamiento se pueden tomar medidas preventivas o correctivas ante eventos que puedan causar daño.

Para evaluar los riesgos a los que está expuesta la empresa T&S COMP. Tecnología y Servicios S.A.S, se utilizará el análisis cuantitativo.

TABLA 1
PROBABILIDAD DE OCURRENCIA

Valor	Criterio	Frecuencia	Descripción
1	Raro	Nunca ha ocurrido.	El evento puede suceder en situaciones extrañas.
2	Improbable	Una vez en el último año.	El evento puede suceder en cierto momento.
3	Posible	Una vez por semestre.	El evento posiblemente podría suceder en cierto momento.
4	Probable	Una vez por mes.	El evento probablemente sucederá en la mayoría de las situaciones.

5	Frecuente	Varias veces en el día.	El evento ocurrirá en la mayoría de las situaciones.

TABLA 2
IMPACTO DE RIESGO

Valor	Criterio	Descripción
1	Insignificante	Si el evento llega a ocurrir, tendría consecuencias mínimas para la empresa.
2	Menor	Si el evento llega a ocurrir, tendría consecuencias bajas para la empresa.
3	Moderado	Si el evento llega a ocurrir, tendría consecuencias medianas para la empresa.
4	Mayor	Si el evento llega a ocurrir, tendría consecuencias altas para la empresa.
5	Catastrófico	Si el evento llega a ocurrir, tendría consecuencias desastrosas para la empresa.

Los criterios de valoración del riesgo para evaluar su criticidad de acuerdo con la siguiente ecuación:

Riesgo = Impacto * Probabilidad de Ocurrencia

TABLA 3
VALORACIÓN DEL RIESGO

	Probabilidad de ocurrencia				
Impacto	**Raro**	**Improbable**	**Posible**	**Probable**	**Frecuente**
Insignificante	1	2	3	4	5
Menor	2	4	6	8	10
Moderado	3	6	9	12	15
Mayor	4	8	12	16	20
Catastrófico	5	10	15	20	25

Una vez valorados los riesgos de acuerdo a cada amenaza encontrada en T&S COMP. Tecnología y Servicios S.A.S, se establecen niveles de aceptación de acuerdo a las categorías determinadas en la tabla 16 y tomando como referencia la norma ISO 27005 Anexo E.

TABLA 4
NIVELES DE ACEPTACIÓN DEL RIESGO

Nivel de aceptación	Valor
Inaceptable	15 - 25
Moderado	5 - 14
Aceptable	1 - 4

La alta gerencia de T&S COMP. Tecnología y Servicios S.A.S decidió tomar una acción inmediata frente a las zonas de riesgos inaceptables ya que se deben trabajar mediante planes de tratamiento de riesgo y los controles establecidos para mitigarlos y mejorar la seguridad de sus recursos.

VII. PLAN DE TRATAMIENTO DE RIESGOS

El plan de tratamiento de riesgos, por medio de la implementación de controles busca disminuir el impacto sobre la infraestructura informática, los procesos en donde se maneja información confidencial y en especial sobre la Confidencialidad, Integridad y Disponibilidad de la información.

Se tienen en cuenta las siguientes medidas de tratamiento:

- Eliminar el riesgo: Tomar las medidas encaminadas para impedir su materialización.
- Mitigar el riesgo: Tomar las medidas para disminuir tanto la probabilidad (medidas de protección), como el impacto (medidas de protección).
- Transferir el riesgo: Reducir el riesgo a través del traspaso de las pérdidas, como en el caso de un contrato de seguros, donde existe un riesgo compartido.
- Aceptar el riesgo: Aceptar el riesgo tolerable, es decir el riesgo residual que aún se mantiene.[3]

La implementación de los controles, es en base a la norma ISO 27001:2013 en su Anexo A, de acuerdo a sus objetivos de control y el manejo de buenas prácticas, los riesgos que se deben tratar de inmediato son los que se encuentran como "Inaceptable", se sugiere que se realice una validación de los controles, que permita mantener el riesgo o mitigarlo, para facilitar la toma de decisiones, con un mínimo de recursos que genere algún costo adicional a la empresa.

[3]DEPARTAMENTO NACIONAL DE PLANEACIÓN. Guía metodológica para la administración de riesgos del SGSI. [online]. [Consultado 15 de febrero de 2017]. Disponible en: https://colaboracion.dnp.gov.co/CDT/DNP/SE-G02%20Gu%C3%ADa%20metodol%C3%B3gica%20para%20la%20admon%20de%20riesgos%20del%20SGSI.Pu.pdf?

Teniendo en cuenta la información anterior, se determina por cada riesgo, el control que debe implementarse para determinar la opción de tratamiento según sea el caso, eliminar el riesgo, mitigar el riesgo, transferir el riesgo y aceptar el riesgo, asociando el control y a su vez una recomendación de tratamiento según el tipo de riesgo al cual la empresa se esté enfrentando y se vean comprometidos los objetivos de la empresa.

En la mayoría de los casos, se busca mitigar los riesgos, evitando que lleguen a materializarse, que el daño sea mayor y afecte considerablemente a la empresa. Cuando por la Alta Gerencia decide eliminar el riesgo, se generan costos altos, que la empresa no estaría dispuesta a pagar, teniendo en cuenta que en su presupuesto no tienen contemplados riesgos asociados con la Seguridad de la Información, se conlleva a tomar otras medidas que les generen un menor costo, que no elimine del todo el riesgo pero que pueda impedir su materialización.

Algunas acciones que permiten controlar o reducir los riesgos presentados, se encuentran por medio de auditorías y programas de verificación de cumplimiento para tener un seguimiento de los controles y su debida implementación. Ésta es la única forma de mantener un control efectivo de los riesgos de Seguridad de la Información que afectan directamente los objetivos de la empresa.

VIII. CONTROLES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La familia de normas ISO 27000 define que la seguridad de la información se establece mediante la implementación de una serie de controles entre los que se encuentran políticas, prácticas, procedimientos y la definición de una estructura organizativa. Estos controles necesitan ser establecidos para asegurar que los objetivos de seguridad específicos, que se han fijado para una determinada organización, se cumplan.

Fig. 1. Dominios 27001:2013[4]

Políticas de la Seguridad de la Información A5. T&S COMP. Tecnología y Servicios S.A.S tiene unas políticas definidas y socializadas, pero no les realizan el seguimiento, teniendo como consecuencias el incumplimiento por parte de los empleados, proveedores y clientes de sus obligaciones interpuestas en las políticas de seguridad.

Se recomendó actualizar las políticas existentes, y realizar una verificación de lo que se está cumpliendo, con el fin de mantener eficacia continua.

Organización de la seguridad de la información A6. Teniendo en cuenta que es una empresa pequeña, está designado el Director de TI, quien tiene la responsabilidad de velar por la seguridad de la información, en relación a los interesados (usuarios, Proveedores y clientes), quienes son los que están involucrados en los procesos de la empresa, definiendo los roles y responsabilidades de la seguridad de la información.

Se recomendó realizar seguimiento a los roles y responsabilidades que cada persona de la empresa debe cumplir, para dar acatamiento a las políticas de la organización, establecer un contacto directo con las autoridades pertinentes a la seguridad de la información para tener una mejor asesoría.

Seguridad de los recursos humanos A7. Antes de asumir el empleo, se realiza revisión de antecedentes y en algunos casos visita domiciliaria. Durante la ejecución del empleo, de acuerdo a las charlas de concientización a los empleados, se les explica la importancia de la seguridad de la información en cada una de sus labores. En la terminación y cambio de empleo, se establece en el contrato inicial, el acuerdo de confidencialidad durante la ejecución del empleo y en la terminación del mismo.

Se recomienda, por parte de la alta gerencia, exigir a todos los empleados y contratistas la aplicación de la seguridad de la información, llevando documentado el seguimiento al cumplimiento de las políticas de seguridad de la información.

Gestión de activos A8. Responsabilidad por los activos: la empresa cuenta con un inventario de los activos físicos de la empresa y de algunos activos de información, sin embargo, no está actualizado, teniendo varios activos que ya no están en uso y que ya no son vitales para la empresa.

En la empresa no manejan una clasificación e identificación de los activos, además el inventario esta desactualizado, por lo tanto, no permite conocer el nivel de seguridad de acuerdo a la Confidencialidad, Integridad y Disponibilidad.

[4] TCPSI. Dominios de la norma ISO 27001:2013 [Online]. [Consultado 21 de enero de 2017]. Disponible en: http://www.tcpsi.com/vermas/iso_27001.htm

Se recomienda actualizar los inventarios de los activos de información, clasificándolos e identificándolos, según su Confidencialidad, Integridad y Disponibilidad, para determinar su nivel de criticidad e implementar los controles de acuerdo al objetivo de control de la norma ISO 27001:2013.

Control de acceso A9. En los requisitos del negocio para el control de acceso se cumplen con las políticas de control de acceso. Todos los empleados deben registrar su entrada en una planilla y a su vez las personas que son externas a las instalaciones. Cada empleado es responsable de la persona externa que lo acompaña. En cuanto al acceso a las redes y servicios, están restringidos los ingresos a determinados sitios en todas las terminales de la empresa T&S COMP. Tecnología y Servicios S.A.S.

Para la gestión de acceso a usuarios se manejan perfiles, no todos los empleados tienen los mismos privilegios y los únicos que tiene acceso a todo es la alta gerencia y la dirección de tecnología.

Se recomienda establecer una política de control de acceso en donde se verifique la calidad de las contraseñas, éstas son responsabilidad de cada usuario y son intransferibles. Se verifican los roles asignados a cada uno de los perfiles y se realiza un seguimiento a los perfiles con más privilegios para evitar incidentes de seguridad de la información.

Criptografía A10. Son implementados los controles criptográficos para los discos de réplica en tiempo real del histórico de la información, el cual se realiza semanalmente, de esta manera se garantiza que la información está segura ante cualquier eventualidad que se pueda presentar, teniendo un respaldo de la misma y garantizando la continuidad del negocio.

Se recomienda cumplir con la implementación de los controles criptográficos en donde se encuentre la información vital de la empresa con accesos restringidos y asignados por el coordinador IT, quien será el responsable de realizar el seguimiento al cumplimento de los controles.

Seguridad física y del entorno A11. En las instalaciones de T&S COMP. Tecnología y Servicios S.A.S no cuentan con áreas de acceso restringido, la única parte que se tiene acceso restringido es el datacenter, el cual tiene acceso biométrico para el coordinador IT y la alta gerencia. Para la seguridad física de las instalaciones, cuentan con CCTV y empresa de monitoreo.

Se recomienda la implementación de los objetivos de control de seguridad física y del entorno, en donde se realicen mantenimientos preventivos a todos los equipos cada 6 meses, llevar un control de ingreso a las áreas restringidas de las instalaciones para que personal no autorizado no ingrese a esas zonas sin los permisos pertinentes. También se debe establecer un monitoreo de los equipos y activos que se encuentren fuera de las instalaciones, garantizando que el personal haga un buen uso de los activos y no perjudique a la empresa.

Seguridad de las operaciones A12. Para los procedimientos operaciones y responsabilidades se tienen definidos algunos procesos de gestión de proyectos, pero no se encuentran documentados. Se realizan copias de seguridad en discos duros semanalmente con réplica en tiempo real. Los discos están cifrados y están almacenados en el datacenter en donde cuentan con control de acceso biométrico.

Se recomienda establecer la política de Seguridad en las operaciones en donde se determinen y se documenten todos los procedimientos. En cuanto a cambios que se generen en la organización, realizar el seguimiento al uso de los recursos y determinar la capacidad de la infraestructura tecnológica. Además, se debe realizar las pruebas de vulnerabilidades cada 3 meses, para establecer las falencias y poder mitigar las amenazas presentadas y establecer auditorias para detectar los posibles eventos de seguridad que se estén presentando en la empresa T&S COMP. Tecnología y Servicios S.A.S.

Seguridad de las comunicaciones A13. Para la gestión de la seguridad de redes, cuentan con controles como: Cada 90 días el sistema ordena cambiar las contraseñas directamente por el dominio, a cada empleado se le asigna una contraseña y se estipula que es intransferible, con único uso y responsabilidad de cada usuario, cada ingreso al sistema queda grabado en el directorio activo y se recomienda tener claves sólidas con caracteres alfanuméricos.

Se recomienda establecer políticas de seguridad de las comunicaciones, en donde existan controles para la transferencia de la información, evitando perdidas de ésta. También se debe exigir el cumplimiento de los acuerdos de confidencialidad. Se sugiere bloqueo de acceso de contenidos pornográficos, y descargas no autorizadas, y establecer la segmentación de la red.

Adquisición, desarrollo y mantenimiento de sistemas A14. Los requisitos de seguridad de la información son establecidos por parte de los clientes en donde se desarrollan los proyectos. Por esta razón, teniendo en cuenta que la empresa trabaja por medio de procesos licitatorios con el estado, la información que manejan es de alta confidencialidad.

El Departamento de Sistemas debe contar con un grupo de personas el cual debe autorizar la creación, adaptación o adquisición de software. Además, debe estar en constante monitoreo para establecer los mantenimientos preventivos y actualizaciones pertinentes a los sistemas de información; este monitoreo se debe realizar cada 3 meses, dirigido por el Coordinador IT y con la compañía de la Alta Gerencia.

Relaciones con los proveedores A15. Política de seguridad de la información para las relaciones con proveedores, Se acordará con el proveedor y se documentarán los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de T&S COMP. Tecnología y Servicios S.A.S.

Cada servicio con proveedor deberá tener con un supervisor encargado de revisar y auditar la prestación de servicios de proveedores, garantizando el cumplimiento de sus obligaciones contractuales.

Gestión de incidentes de seguridad de la información A16. La priorización del tratamiento de los incidentes se realiza conforme a la criticidad de la Información. El responsable de la información debe definir los eventos considerados como críticos junto con sus respectivas alertas y registros de seguridad de la información, los cuales deberán ser generados. Éstos deben ser activados, vigilados, almacenados y revisados permanentemente, y las situaciones no esperadas deben ser reportadas de manera inmediata al equipo de respuesta a Incidentes.

Los empleados deben estar informados del proceso disciplinario que se llevará a cabo en caso de incumplimiento de la Política de Seguridad de la Información o alguno de los elementos que la soportan. En cualquier caso, se hará un seguimiento de acuerdo con los procedimientos establecidos para el manejo de incidentes de seguridad.

Aspectos de seguridad de la información de la gestión de continuidad de negocio A17. La empresa T&S COMP. Tecnología y Servicios S.A.S, cuenta con algunos controles para la gestión de continuidad del negocio, entre lo que se encuentra lo siguiente:

TABLA 5
MANTENIMIENTO PREVENTIVO EQUIPO INFORMÁTICO

Mantenimiento preventivo por equipo informático		
Equipo	**Acción preventiva/correctiva**	**Responsable**
Computadores de Escritorio y Portátiles	Revisión, limpieza interna y externa de todos los componentes. Revisión de virus	Departamento de Sistemas en coordinación con el Departamento de Servicio quien asigna el técnico para la ejecución de la acción.
Impresoras	Revisión, limpieza y lubricación interna y externa de todos los componentes.	Departamento de Sistemas en coordinación con el Departamento de Servicio quien asigna el técnico para la ejecución de la acción.
Servidores	Se realiza un monitoreo a través de acciones manuales en cada servidor. Revisión, limpieza interna y externa de todos los componentes.	Departamento de Sistemas

Cumplimiento A18. Deben establecerse procedimientos apropiados para asegurar el cumplimiento con las restricciones de carácter legal en el uso de material que puede estar sujeto a derechos de propiedad intelectual tales como derechos de autor y derechos de diseño.

Identificación de la legislación aplicable y los requisitos contractuales: todos los requisitos pertinentes, legislativos estatutarios, reglamentarios y contractuales, y el planteamiento de la entidad para cumplir con estos requisitos deberán estar explícitamente identificados, documentados y protegidos al día para cada sistema de información y la organización.

El Departamento de Sistemas deberá comprobar periódicamente el cumplimiento de los procedimientos de procesamiento de la información dentro de su área de responsabilidad con las políticas de seguridad, las normas y otros requisitos de seguridad.

IX. RESULTADOS

¿Cómo se puede establecer la integridad, disponibilidad y confidencialidad de la información en un modelo de negocio orientado a la prestación de servicios tecnológicos?

Para establecer la integridad, disponibilidad y confidencialidad de la información en un modelo de negocio orientado a la prestación de servicios tecnológicos, se deben adoptar procesos adecuados para la planeación, implementación, mantenimiento y mejora del SGSI, de acuerdo a la norma ISO 27001:2013

Por medio del diseño del Sistema de Gestión de Seguridad de la Información, conociendo como es el manejo de la información en cada uno de los procesos de la empresa T&S COMP. Tecnología y Servicios S.A.S, se determinaron cuáles son las vulnerabilidades y posibles amenazas, identificando los diferentes riesgos que afectan a la empresa para evitar que se materialicen. Por esto, por medio de mejores prácticas fomentadas desde la alta gerencia, se crea un ambiente de cultura de Seguridad de la Información a todas las partes interesadas en el desarrollo de la prestación de su servicio.

Teniendo en cuenta que el modelo de negocio está orientado a la prestación de servicios tecnológicos, en donde la información es un activo vital, que puede ser alterado, divulgado y no disponible, es necesario aplicar los diferentes planes de tratamiento apoyados en los controles de la norma ISO 27001:2013. Para tener un adecuado uso y manejo de la información vital de la empresa, se debe tener en cuenta que estos servicios son ofrecidos en su mayoría a empresas del estado y es de vital importancia poder brindar seguridad y confianza a los clientes, garantizando el buen uso de la información brindada por las partes.

X. CONCLUSIONES

Las Pequeñas y medianas empresas, como T&S COMP. Tecnología y Servicios S.A.S, con la innovación tecnológica, se enfrentan a riesgos que pueden generar daños irreparables

en el desarrollo de las actividades de las organizaciones. Con el diseño del Sistema de Gestión de Seguridad de la Información en la empresa, ayudó a establecer mecanismos para la protección de los activos de información y tomar precauciones para asegurar los sistemas que procesan esa información.

Para el diseño de Sistema de Gestión de Seguridad de la Información en T&S COMP. Tecnología y Servicios S.A.S, se contó con la participación de la alta dirección y el respaldo de todos los procesos, teniendo en cuenta que son los principales interesados en que se incluyan estándares de Seguridad Informática necesarios. Con esto, tanto sus funcionarios, clientes y proveedores tienen la certeza que se utilizan buenas prácticas para la protección de su información logrando aumentar su confianza en la empresa.

La Seguridad de la Información es fundamental en los diferentes procesos que se manejan en la empresa, sin embargo, el personal no toma el tema de la seguridad de la información como importante y no da prioridad a los activos de información que son vitales para la empresa. Con el diseño del Sistema de Gestión de Seguridad de la Información, ayudó a establecer procedimientos y buenas prácticas para manejo óptimo para el desarrollo de las actividades de la empresa y a cumplir con los requisitos legales teniendo en cuenta la Confidencialidad, Integridad y Disponibilidad de su información.

El análisis de riesgos contribuyó a detectar las amenazas a las que la organización está expuesta, frente a la inadecuada gestión de conocimiento de sus activos de información, lo que les permitió reconocer los riesgos a los que se enfrentan y el impacto que puede originar si se materializan. Para los riesgos que resultaron inaceptables, se enfocaron esfuerzos para realizar una acción inmediata con el fin de generar controles para mitigarlos y crear valor a los activos de información de cada uno de los procesos.

La gestión efectiva de la Seguridad de la Información debe estar inmersa desde la alta gerencia, empleados, clientes y proveedores, en donde cada uno tiene un rol importante para que el cumplimiento de controles y políticas sea todo un éxito. Asimismo, se garantiza el buen uso de la información, mitigando en lo posible todos los riesgos que se generan en los diferentes procesos y saber cómo actuar, para tener una buena toma de decisiones, llegar asumir los riesgos residuales que sean mínimos, y mantener un buen estado de seguridad de la información, con un monitoreo constante.

REFERENCIAS

[1] PORTAFOLIO, 'La seguridad informática se contrajo 15 % en ventas'. [Online] [Consultado el 25 de abril de 2016]. http://www.portafolio.co/negocios/la-seguridad-informatica-se-contrajo-15-ventas

[2] T&S COMP. TECNOLOGÍA Y SERVICIOS S.A.S. Generalidades de la empresa. [Online] [Consultado el 25 de abril de 2016]. http://tyscomp.com/nosotros/

[3] DEPARTAMENTO NACIONAL DE PLANEACIÓN. Guía metodológica para la administración de riesgos del SGSI. [online]. [Consultado 15 de febrero de 2017]. Disponible en: https://colaboracion.dnp.gov.co/CDT/DNP/SE-G02%20Gu%C3%ADa%20metodol%C3%B3gica%20para%20la%20admon%20de%20riesgos%20del%20SGSI.Pu.pdf?

[4] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, ISO 27000. [Online]. [Consultado 25 de abril de 2016]. Disponible en: http://www.iso27000.es/download/doc_iso27000_all.pdf

[5] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, ISO 27000. [Online]. [Consultado 25 de febrero de 2017]. Disponible en: http://www.iso27000.es/glosario.html

[6] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO 31000:2011 - Risk management. Principles.

[7] MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Guía para la Gestión y Clasificación de Activos de Información. Clasificación de activos de la información.

[8] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Glossary of Key Information Security Terms. [Online]. [Consultado 17 de diciembre de 2016]. Disponible en: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

[9] DEPARTAMENTO NACIONAL DE PLANEACIÓN, Guía metodológica para la administración de riesgos del SGSI [online]. [Consultado 15 de febrero de 2017]. Disponible en: https://colaboracion.dnp.gov.co/CDT/DNP/SE-G02%20Gu%C3%ADa%20metodol%C3%B3gica%20para%20la%20admon%20de%20riesgos%20del%20SGSI.Pu.pdf?

[10] ALCALDÍA MAYOR DE BOGOTÁ. Ley 527 de 1999 [Online]. [Consultado 31 de enero de 2016]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276

[11] ALCALDÍA MAYOR DE BOGOTÁ. Ley Estatutaria 1581 de 2012 [Online]. [Consultado 20 de diciembre de 2016]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

[12] ALCALDÍA MAYOR DE BOGOTÁ. Ley Estatutaria 1581 DE 2012 [Online]. [Consultado 20 de diciembre de 2016]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981